Acquisition Directorate
Research & Development Center

Report No. CG-D-09-09

MDA DS COI Spiral 3 – NOA, SILO and ABAC - Final Report

Distribution Statement:

This document is available to the U.S. public through the National Technical Information Service, Springfield, VA 22161.

June 2009

Homeland Security

NOTICE

This document is disseminated under the sponsorship of the Department of Homeland Security in the interest of information exchange. The United States Government assumes no liability for its contents or use thereof.

The United States Government does not endorse products or manufacturers. Trade or manufacturers' names appear herein solely because they are considered essential to the object of this report.

This report does not constitute a standard, specification, or regulation.

Donald F. Cundy
Executive Director
United States Coast Guard
Research & Development Center
1 Chelsea Street
New London, CT 06320-5506

Technical Report Documentation Page

1. Report No.
CG-D-09-09

2. Government Accession Number

3. Recipient's Catalog No.
N/A

4. Title and Subtitle
MDA DS COI Spiral 3 – NOA, SILO and ABAC - Final Report

5. Report Date
June 2009

6. Performing Organization Code
Project No. 2417

7. Author(s)
Jay Spalding, Jim Harmon, Alistair Nicol, and Mark MacKinnon

8. Performing Organization Report No.
R&DC UDI No. 903

9. Performing Organization Name and Address

U.S. Coast Guard
Research and Development Center
1 Chelsea Street
New London, CT 06320

SAIC
23 Clara Drive, Suite 206
Mystic, CT 06355-1959

10. Work Unit No. (TRAIS)
N/A

11. Contract or Grant No.
Contract HSCG32-05-D-R00010/
Task Order HSCG32-08-J-100041

12. Sponsoring Organization Name and Address
U.S. Department of Homeland Security
United States Coast Guard
Commandant (CG-262)
Washington, DC 20593-0001

13. Type of Report & Period Covered
Final

14. Sponsoring Agency Code
Commandant (CG-262)
U.S. Coast Guard Headquarters
Washington, DC 20593-0001

15. Supplementary Notes
The R&D Center's technical point of contact is Mr. Jay Spalding, 860-271-2687, Jay.W.Spalding@uscg.mil.

16. Abstract (MAXIMUM 200 WORDS)

The purpose of this report is to document United States Coast Guard (USCG) Research and Development (R&D) efforts in support of the Maritime Domain Awareness Data Sharing Community of Interest (MDA DS COI) Spiral 3 Project. The project focuses on sharing the sensitive data associated with Notice of Arrival (NOA) messages and the Single Integrated LookOut (SILO) list in a net-centric Web-services environment. It documents the background of the efforts leading up to the project, the technological hurdles faced in achieving a solution, and the policy and collaborative challenges experienced during the project. The COI, which included the Coast Guard and other Department of Homeland Security (DHS) agencies, laid the foundation for a complete paradigm shift in the protection of sensitive data, and enabled its exposure in an enterprise network environment without compromising the information.

This report summarizes the end result of Spiral 3 and describes the transition to a new framework for future development.

17. Key Words
ANOA
SILO
ABAC
NCES
MDA
MIEM
SANS

18. Distribution Statement
Document is available to the U.S. public through the National Technical Information Service, Springfield, VA 22161.

19. Security Class (This Report)
UNCLASSIFIED

20. Security Class (This Page)
UNCLASSIFIED

21. No of Pages
83

22. Price
N/A

This page intentionally left blank.

EXECUTIVE SUMMARY

This project is part of a series of efforts executed in response to Department of Homeland Security (DHS) requirements for increased awareness of the maritime domain and the threats posed within. A Maritime Security Policy was established in December 2004, delineated in the National Security Presidential Directive (NSPD) 41/Homeland Security Presidential Directive (HSPD) 13, which defined maritime domain awareness (MDA) and dictated the need for a national strategy for achieving it. The directive further dictated interagency participation and the effective Government-wide sharing of information, to include state and local agencies.

The National Plan to Achieve MDA, a by-product of the Maritime Security Policy, established the national maritime common operating picture (COP) as the primary means of displaying shared data and focused on net-centricity to achieve its goal. The MDA Data Sharing Community of Interest (DS COI) was established to leverage net-centric Web-based technology and capabilities to address complex data sharing requirements among multiple agencies. It was chartered in March 2006 and includes Department of Defense (DoD) and DHS, who are the governing authorities, as well as other Federal agencies, law enforcement, international governments, and members of the maritime industry. Its purpose is to implement the national net-centric data sharing strategy in order to improve maritime security. As the lead maritime agency in DHS , the Coast Guard has exercised a lead role in achieving the COI's goals.

Using the Coast Guard's Nationwide Automatic Identification System (NAIS) data in Spirals 1 and 2, the COI proved that unclassified information could indeed be shared across an enterprise network, making it available to any consumer who needed the data and had access to the network. The goal of Spiral 3 was to prove that sensitive data, normally controlled by the provider, could be made available to an enterprise network with the necessary access controls to avoid inadvertent disclosure to unauthorized recipients. For this purpose, Attribute Based Access Control (ABAC) was selected as the access control technology for the project. For the data sources, the Coast Guard's Notice of Arrival (NOA) data and the Single Integrated LookOut (SILO) list from the Office of Naval Intelligence (ONI) were selected as data sources. NOA data, referred to in the industry as Advance NOA (ANOA), contains the information required of all vessels entering or departing ports in the United States about their intended arrival and departure dates and times, cargo, and crew/passenger lists. Crew/passenger lists contain names, social security or passport numbers, and other personally identifiable information (PII), which is protected by law from unauthorized use or disclosure. SILO data contains aggregated information about vessels determined to be of interest by intelligence and operational organizations and is normally classified or highly sensitive. Exposing either data source to an enterprise network would require a sophisticated access control method that ensured that any individual with access to the network also had the necessary credentials to access the data.

The Pilot Technical Working Group (PTWG), responsible for technical development within the MDA DS COI, worked closely with the data stewards of ANOA and SILO to determine the best solution. They also worked closely with the Defense Information Systems Agency (DISA) who manages the Net-Centric Enterprise Service (NCES), the enterprise network through which consumers access AIS data and the intended service for ANOA and SILO data as well.

For the ABAC solution, the COI initially chose the Net-Centric Enterprise Services (NCES) Security Service because it already existed and appeared to provide the necessary elements for access control.

However, it was determined the NCES Security Service was not able to satisfy the level of decision necessary for multiple data sets with different attribute policies, so the PTWG pursued a more advanced solution. An architecture was designed and developed as a prototype, and the data producers within the COI defined data sharing policy for their data in order to build a working ABAC model. During the ABAC development process, the PTWG had to focus its efforts on NCES Managed Services Platform (MSP) transition, delaying completion of the ABAC model. A proof of concept implementation was developed early in 2009 based on the requirements developed and ABAC for the ANOA and SILO services can now be demonstrated.

For ANOA, the Coast Guard's Maritime Awareness Global Network (MAGNet) Program (CG-262) is the data steward for NOA data. MAGNet receives NOA data from the Ship Arrival Notification System (SANS) database and makes it available to its users. For Spiral 3, the Coast Guard team, consisting of CG-26, the Operations Systems Center (OSC), and the Coast Guard Research & Development Center (R&DC), developed a plan for publishing NOA data to the OSC Service Oriented Architecture (SOA) initiative for further distribution to NCES as ANOA service. The key elements that had to be determined included the schema, the definition of attributes for access control, and what level of service would be provided for ANOA. Initially, the Maritime Information Exchange Model (MIEM) schema was chosen for ANOA because of its broad acceptance within the COI. However, it proved unwieldy and rigid for SANS-based data. So, the decision was made for MAGNet to provide ANOA data in the SANS schema to the OSC, through the Enterprise Service Bus (ESB), and on to NCES. ANOA data is now being published on NCES without PII. Access control for ANOA with PII requires more work on defining and controlling role-based access for messaging channels and ABAC for query requests.

For SILO, policy would prove too challenging for a short-term solution because of classification issues. Exposing vessel of interest data can only be authorized if the data can be "sanitized" (classified data removed), and an approved method for transferring data from a classified domain to an unclassified domain exists. To lay the foundation for a cross-domain solution, ONI wanted to expose unclassified AIS data from the Non-secure Internet Protocol Router Network (NIPRNET) to the Secret Internet Protocol Router Network (SIPRNET). Working with DISA, the PTWG leveraged the Cross Domain Web Services Gateway (CDWSG), already established for other applications, to pass AIS data to the SIPRNET. However, they were still waiting for the Public Key Infrastructure (PKI) certificates as of the Spiral 3 demonstration in March 2009. The CDWSG remains viable for the cross-domain transfer of information, but a classified-to-unclassified solution requires more work before being applied for SILO data.

Spiral 3 developments were successfully demonstrated on 31 March 2009. ANOA data is being published without PII and is accessible to any authorized consumer, via Common Access Card (CAC) or PKI certificate. The COI also demonstrated that the ABAC concept for sensitive data was feasible with properly defined attributes.

As a result of this project, a wider variety of mission-critical MDA data is accessible by increasing numbers of consumers. Federal agencies (e.g., DoD, DHS, Intelligence Community, etc.), law enforcement agencies at the Federal, state, and local levels, international partners, and industry partners have discovered that net-centric Web services facilitate greater situational awareness and enhance mission accomplishment. Furthermore, the COI has developed experience and knowledge of data sharing complexities and solutions unprecedented within the DoD and DHS communities. This expertise will help solve new technological hurdles and bring a focused perspective to solving the challenges that lay ahead.

TABLE OF CONTENTS

EXECUTIVE SUMMARY .... **V**

LIST OF FIGURES .... **IX**

LIST OF TABLES .... **X**

LIST OF ACRONYMS/TERMS .... **XI**

1 PURPOSE **1**

2 BACKGROUND **1**

2.1 Establishment of the MDA DS COI 1
2.1.1 MDA DS COI Organization 2
2.1.2 Data Management Working Group 2
2.1.3 Policy Working Group 2
2.1.4 Pilot Technical Working Group 3
2.2 Net-centric Data Sharing/Spiral Projects 3
2.2.1 Spiral 1 Pilot Project 3
2.2.2 Spiral 2 Pilot Project 5

3 SPIRAL 3 .... **6**

3.1 ABAC 7
3.1.1 Technical Approach for Implementing an ABAC Solution 7
3.1.2 ABAC Governance 8
3.1.3 ABAC Architecture 9
3.1.4 Data Access Through ABAC 10
3.2 ANOA 12
3.2.1 Technical Approach for Sharing ANOA Data 12
3.2.2 ANOA Governance 13
3.2.3 NCES Transition and ANOA 13
3.2.4 ANOA Schema 14
3.2.5 ANOA Architecture 15
3.3 SILO 16
3.3.1 Technical Approach for Sharing SILO Data 17
3.3.2 SILO Governance 18
3.3.3 SILO Architecture 18
3.3.4 Cross-domain Solution 19
3.4 Spiral 3 Demonstration 20

TABLE OF CONTENTS (Continued)

4 LESSONS LEARNED 24
4.1 Technical 24
4.2 Governance 24
4.3 Cultural 24
4.4 Implementation 25
5 RECOMMENDATIONS 25
6 SUMMARY 26
APPENDIX A. MDA DS COI A-1
APPENDIX B. DATA SHARING POLICY FRAMEWORK B-1
APPENDIX C. NOTICE OF ARRIVAL (NOA) C-1
APPENDIX D. SPIRAL 3 SCHEMAS D-1
APPENDIX E. SERVICES E-1

LIST OF FIGURES

Figure 1. MDA DS COI governance. 2
Figure 2. Net-centric enterprise publish/subscribe process. 4
Figure 3. MDA DS COI Spiral 1 pilot high-level architecture. 4
Figure 4. ABAC architecture, January 2008. 8
Figure 5. ANOA ABAC architecture, March 2009. 9
Figure 6. Users of ANOA data. 10
Figure 7. Channel selected showing a vessel with an ANOA. 11
Figure 8. Basic vessel information with link to Advance Notice of Arrival Query. 11
Figure 9. ANOA architecture. 15
Figure 10. ANOA publishing architecture. 16
Figure 11. ANOA Federated Search architecture. 17
Figure 12. Phase 1 SILO architecture. 19
Figure 13. Data flow through NCES. 21
Figure 14. Ship with ANOA tag (HATSU EXCEL). 21
Figure 15. ANOA with arrival port (green) and previous ports (grey). 22
Figure 16. Ship with vessel of interest (VOI) tag (CARNIVAL PARADISE). 23
Figure 17. ABAC return of the crew information (PII) to a Law Enforcement user. 23
Figure A-1. MDA DS COI governance. A-3
Figure A-2. Net-centric coalition of the willing. A-5
Figure A-3. History of the MDA DS COI. A-6
Figure C-1. Extraction from Title 33, CFR, Part 160 describing the required contents of an NOA. C-1
Figure D-1. Relationship among XSDs, XML instances, data providers/subscribers, and NCES messaging. D-1
Figure D-2. Basic MIEM message structure. D-2
Figure D-3. Basic ANOA message structure. D-3
Figure D-4. ANOA Notice of Arrival message body. D-4
Figure D-5. ANOA example vessel element detail. D-5
Figure D-6. ANOA example port element detail. D-8
Figure D-7. MIEM – ANOA schema conceptual model. D-9
Figure D-8. SANS e-NOA example message. D-10
Figure D-9. SILO conceptual model. D-13
Figure D-10. Basic SILO message structure. D-14
Figure E-1. NCES service registry website. E-2
Figure E-2. DoD metadata registry website. E-4
Figure E-3. GMMS website. E-6
Figure E-4. MAT website. E-7

LIST OF TABLES

Table B-1. Information sharing framework for USCG-ANOA. B-1
Table B-2. Information sharing framework for ONI-SILO (at the UNCLAS NIPRNET security domain). B-6

LIST OF ACRONYMS/TERMS

ABAC	Attribute Based Access Control
ACTD	Advanced Concept Technology Demonstration
ADS	Anomaly Detection Service
AIS	Automatic Identification System
AMH	Architecture Management Hub
AMRS	Automated Merchant Reporting System
ANOA	Advance Notice of Arrival
AS	Attribute Service
ATA	Actual Time of Arrival
ATD	Actual Time of Departure
Atom	Publishing protocol used as an application-level protocol for publishing and editing Web Resources using HTTP and XML
C&A	Certification and Accreditation
CAC	Common Access Card
CANES	Consolidated Afloat Networks and Enterprise Services
CAPCO	Controlled Access Program Coordination Office
CBP	Custom and Border Protection
CDC	Certain Dangerous Cargo
CDS	Cross Domain Solution
CDWSG	Cross Domain Web Services Gateway
CES	Core Enterprise Services
CFR	Code of Federal Regulations
CIO	Chief Information Officer
CMA	Comprehensive Maritime Awareness
COI	Community of Interest
CONOPS	Concept of Operations
COP	Common Operational Picture
COTS	Commercial Off-the-Shelf
CSV	Comma Separated Value
CT&E	Certification Test and Evaluation
CTK	Conformance Test Kit
CWID	Coalition Warrior Interoperability Demonstration
DAS	Data Augmentation Service
DB	Database
DCI	Director of Central Intelligence
DECC	Defense Enterprise Computing Center
DHS	Department of Homeland Security
DIACAP	DoD Information Assurance Certification and Accreditation Process
DISA	Defense Information Systems Agency
DKO	Defense Knowledge Online
DMWG	Data Management Working Group
DMS	Degrees, Minutes, Seconds
DN	Distinguished Name

LIST OF ACRONYMS/TERMS (Continued)

DoD	Department of Defense
DoDI	DoD Instruction
DOJ	Department of Justice
DON	Department of the Navy
DS	Data Sharing
DSG	Data Synch Guard
ebXML	e-business XML
ECA	External Certification Authority
ECB	Early Capability Baseline
ECS	Executive Steering Committee
EDMO	Enterprise Data Management Office
EESB	Enterprise Engineering Services Branch
e-NOA	Electronic Notice of Arrival
e-NOA/D	Electronic Notice of Arrival/Departure
ESB	Enterprise Service Bus
ETA	Estimated Time of Arrival
ETD	Estimated Time of Departure
ETT	Emerging Technologies Team
FOUO	For Official Use Only
GeoRSS	Geographic RSS
GIG	Global Information Grid
GMII	Global Maritime Intelligence Integration
GMMS	Google Maps Mediation Service
GUI	Graphical User Interface
HAS	Historical Archive Service
HSIN	Homeland Security Information Network
HSPD	Homeland Security Presidential Directive
HTML	HyperText Markup Language
IA	Intelligence Agency
IATO	Interim Authority To Operate
IC	Intelligence Community
ICC	Intelligence Coordination Center
ICE	Immigrations and Customs Enforcement
ID	Identification
IMO	International Maritime Organization
IOC	Interagency Operation Centers
IOT&E	Initial Operational Test & Evaluation
ISM	Information Security Marking
ISSC	International Ship Security Certificate
JCTD	Joint Concept Technology Demonstration
JEDS	Joint Enterprise Discovery Service
JROCM	Joint Requirements Oversight Council
JSON	JavaScript Object Notation

LIST OF ACRONYMS/TERMS (Continued)

KML	Keyhole Markup Language
LAS	Local Attribute Store
LDAP	Lightweight Directory Access Protocol
LEA	Law Enforcement Agency
MAGNet	Maritime Awareness Global Network
MASTER	Maritime Automated SuperTrack Enhanced Reporting
MAT	Metric Analysis Tool
MDA	Maritime Domain Awareness
MDR	Metadata Registry
MIEM	Maritime Information Exchange Model
MIFCLANT	Maritime Intelligence Fusion Center Atlantic
MIFCPAC	Maritime Intelligence Fusion Center Pacific
MMSI	Maritime Mobile Service Identity
MOU	Memoranda of Understanding
MSP	Managed Services Platform
MSSIS	Maritime Security Safety Information System
NAIS	Nationwide Automatic Identification System
NASA	National Aeronautics and Space Administration
NATO	North Atlantic Treaty Organization
NCES	Net-Centric Enterprise Services
NGA	National Geospatial-Intelligence Agency
NGA	Non-Government Agency
NIEM	National Information Exchange Model
NIPRNET	Non-secure Internet Protocol Router Network
NMIC	National Maritime Intelligence Center
NOA	Notice of Arrival
NORAD	North American Aerospace Defense Command
NORTHCOM	Northern Command
NPS	Naval Postgraduate School
NRL	Naval Research Laboratory
NSA	National Security Agency
NSPD	National Security Presidential Directive
NVMC	National Vessel Movement Center
OCE	Operational Condition of Equipment
OCIO	Office of the Chief Information Officer
OGA	Other Government Agency
ONI	Office of Naval Intelligence
ONR	Office of Naval Research
OPNAV	Operational Navy
OSC	Operations Systems Center
OTH	Over the Horizon
PDP	Policy Decision Point
PDS	Policy Decision Service
PEP	Policy Enforcement Point

LIST OF ACRONYMS/TERMS (Continued)

PES	Policy Enforcement Service
PII	Personally Identifiable Information
PKI	Public Key Infrastructure
POR	Program of Record
PTT	Pilot Technical Team
PTWG	Pilot Technical Working Group
PWG	Policy Working Group
QoS	Quality of Service
R&D	Research and Development
R&DC	Research & Development Center
RBAC	Role-based Access Control
RCVS	Robust Certificate Validation Service
RSS	Really Simple Syndication
SAIC	Science Applications International Corporation
SAML	Security Assertion Markup Language
SANS	Ship Arrival Notification System
SCONUM	Ship Control Number
SILO	Single Integrated LookOut
SIPRNET	Secret Internet Protocol Router Network
SME	Subject Matter Expert
SOA	Service Oriented Architecture
SOAP	Simple Object Access Protocol
SPAWAR	Space & Naval Warfare Systems Command
SSC SD	SPAWAR Systems Center San Diego
SSL	Secure Sockets Layer
TSA	Transportation Security Administration
TTL	Time-to-Live
U	Unclassified
U.S.	United States
UCore	Universal Core
UDDI	Universal Description, Discovery and Integration
UDOP	User-defined Operational Picture
USCG	United States Coast Guard
USN	U. S. Navy
VOI	Vessel of Interest
WebTAS	Web-enabled Timeline Analysis System
WS	Web Services
XACML	Extensible Access Control Markup Language
XML	Extensible Markup Language
XSD	XML Schema Definition

1 PURPOSE

The purpose of this report is to document the United States Coast Guard (USCG) Research and Development (R&D) efforts in support of the Maritime Domain Awareness Data Sharing Community of Interest (MDA DS COI) Spiral 3 Project. Spiral 3 sought to improve data sharing accomplishments achieved in Spirals 1 and 2 by adding sensitive data sources and Attribute Based Access Control (ABAC) to ensure against unauthorized disclosure of the data. Advanced Notice of Arrival (ANOA) and Single Integrated LookOut (SILO) were selected as the new data sources because of the sensitive nature of the information within. ANOA is based on the Coast Guard's statutory requirement for a Notice of Arrival (NOA) filed prior to 96 hours of arriving in United States (U.S.) ports. It contains valuable information about the vessel, its cargo, and its crew, including personally identifiable information (PII), which cannot be shared outside the Coast Guard and law enforcement agencies. SILO is an aggregated list of vessels of interest produced by the U.S. Navy's Office of Naval Intelligence (ONI). It includes classified as well as sensitive unclassified data about vessels posing a potential threat to the U.S. This report discusses the background of the MDA DS COI and its associated Spiral projects, the development environment in which this project was executed, and the problems encountered in solving data sharing challenges. Finally, it offers lessons learned and recommendations for future Coast Guard involvement in MDA DS development.

2 BACKGROUND

This project is part of a series of efforts executed in response to Department of Homeland Security (DHS) requirements for increased awareness of the maritime domain and the threats posed within. A Maritime Security Policy was established in December 2004, delineated in the National Security Presidential Directive (NSPD) 41/Homeland Security Presidential Directive (HSPD) 13, which defined MDA and dictated the need for a national strategy for achieving it. The directive further dictated interagency participation and the effective Government-wide sharing of information to include state and local agencies.

2.1 Establishment of the MDA DS COI

The National Plan to Achieve MDA, a by-product of the Maritime Security Policy, established the national maritime common operating picture (COP) as the primary means of displaying shared data and focused on net-centricity to achieve its goal. The MDA DS COI was established to leverage net-centric Web-based technology and capabilities in addressing complex data sharing requirements among multiple agencies (see APPENDIX A). It was chartered in March 2006 and includes Department of Defense (DoD) and DHS, who are the governing authorities, as well as other Federal agencies, law enforcement, international governments, and members of the maritime industry. Its purpose is to implement the national net-centric data sharing strategy in order to improve maritime security. Among others, pertinent COI objectives include the following:

- Compiling and addressing information-sharing requirements for platforms or agencies operating within the MDA environment;
- Defining/implementing a work process for fostering COI-wide data sharing and management methods and capabilities;
- Developing a shared vocabulary (Section 2) in accordance with DoD Net-Centric Data Strategy that is consistent with the data strategy of non-DoD participants;
- Developing repeatable processes that promote community-wide data management and access; and
- Facilitating implementation of net-centric data sharing and Services Oriented Architecture (SOA) across member organizations.

2.1.1 MDA DS COI Organization

The management hierarchy of the MDA DS COI consists of an Executive Board and a Steering Committee. The hierarchy of the COI, including the Working Groups, is shown in Figure 1.

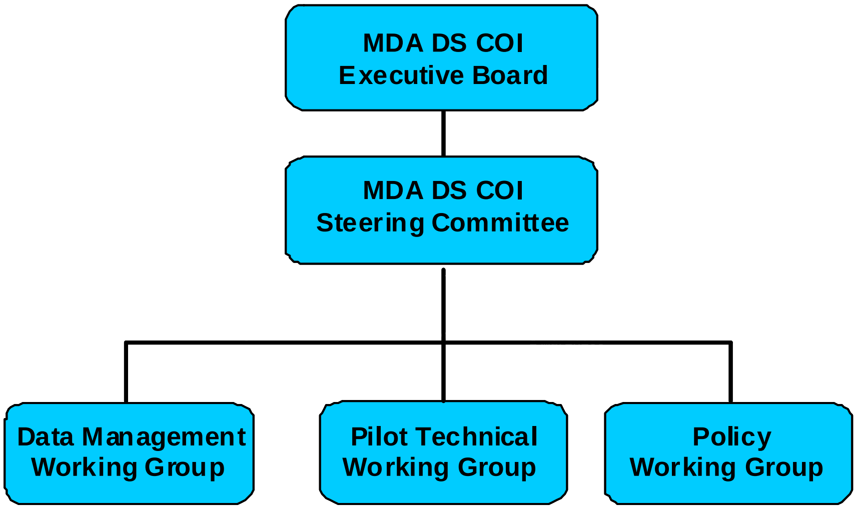


Figure 1. MDA DS COI governance.

- The Executive Board was made up of a senior member each from DoD and DHS and provided advocacy, as required, to secure necessary resources that enabled the COI to meet its mission.
- The Steering Committee was chaired by senior members (O6/GS-15) from DoD and DHS. Their role was to review and adjudicate COI conflicts, advocate for organizational implementation and support, and direct the activities of the working groups.
- The Working Groups were directed by the Steering Committee to address specific actions delineated in DoD Guide 8320.2-G, *Guidance for Implementing Net-Centric Data Sharing*. Group leadership was primarily from DoD and DHS, but came from other departments and agencies as appropriate.

2.1.2 Data Management Working Group

The Data Management Working Group (DMWG) was established in February 2006 to develop the MDA COI Pilot core vocabulary, data models and schemas. The DMWG developed shared vocabulary for the Maritime Domain problem area in accordance with DoD Net-Centric Data Strategy and other Government data management guidance.

2.1.3 Policy Working Group

The Policy Working Group (PWG) reviews issues, writes and recommends policy that deconflicts data sharing issues. Its purpose is to ensure that policy exists to support promulgation of MDA information. The PWG was responsible for establishing the following:

- Business rules/security policies for sharing of personal information;
- NCES governance structure;
- What information could be shared freely;
- What information could be shared only with designated personnel/groups;
- What information could not be shared; and
- What monitoring/testing was required to ensure information sharing policies were met.

2.1.4 Pilot Technical Working Group

The Pilot Technical Working Group (PTWG) was responsible for developing repeatable processes and capabilities to demonstrate COI products (i.e., data vocabulary, enterprise services, user-defined operational picture (UDOP). The PTWG was comprised of Navy,Coast Guard and contractor subject matter experts (SMEs). It was tasked with developing solutions to complex technical problems, which for Spiral 3 included sharing sensitive data with adequate protection from unauthorized disclosure.

2.2 Net-centric Data Sharing/Spiral Projects

The goal of net-centric data sharing is to make data discoverable, accessible, and understandable. To facilitate that goal, the COI executed a series of pilot projects designed to demonstrate the capability to share specific data among a wide cross-section of consumers. These projects were executed as spirals, each building on its predecessor. Spiral 1 and 2 addressed sharing of Automatic Identification System (AIS) and Spiral 3 branched out to other types of MDA vessel related data, the Notice of Arrival and Lookout Lists. While AIS is primarily used for safety of navigation and collision avoidance, the vessel and tracking information provided by AIS makes it useful to DoD and DHS agencies, as well as others within the COI. To validate the net-centric concept, the Net-Centric Enterprise Services (NCES), operated by the Defense Information Systems Agency (DISA), was selected as the medium through which AIS data could be shared. The sensitive nature of ANOA and SILO brought new data sharing challenges to the COI. Figure 2 depicts the net-centric enterprise publish/subscribe process.

2.2.1 Spiral 1 Pilot Project

The goal of the Spiral 1 pilot project was to demonstrate a net-centric data sharing capability in an SOA environment using common vocabularies and schemas. This capability needed to support data exchanges among multiple producers and consumers with a common methodology for exposing, discovering, publishing, and subscribing to unclassified MDA data. The Spiral 1 pilot utilized the DHS Homeland Security Information Network (HSIN) and the DoD NCES Early Capability Baseline (ECB) to implement the services required to expose the data. The DMWG also created an MDA DS COI schema to expose AIS positional data (i.e. location, course, speed, etc.), as well as static data, such as ship's name, Maritime Mobile Service Identity (MMSI), and International Maritime Organization (IMO) number. The PTWG leveraged the DMWG's vocabulary and schema to demonstrate an unclassified data sharing capability using NCES net-centric services for discovery, via the NCES Content Discovery/Federated Search Service, and for access via the NCES Messaging Service (See Figure 3.)

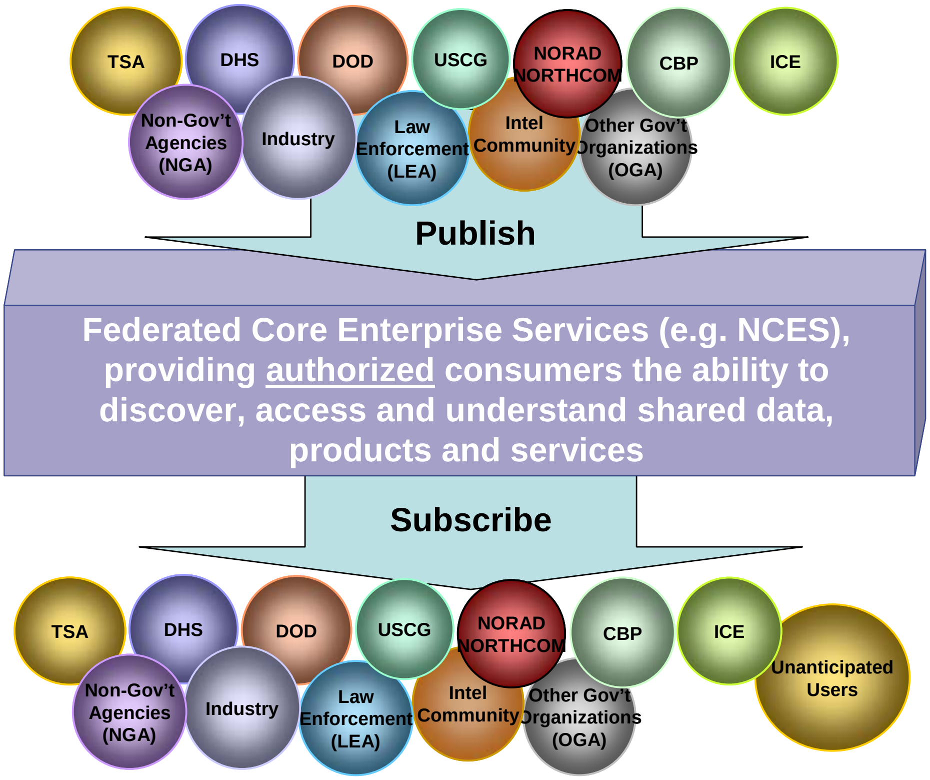


Figure 2. Net-centric enterprise publish/subscribe process.

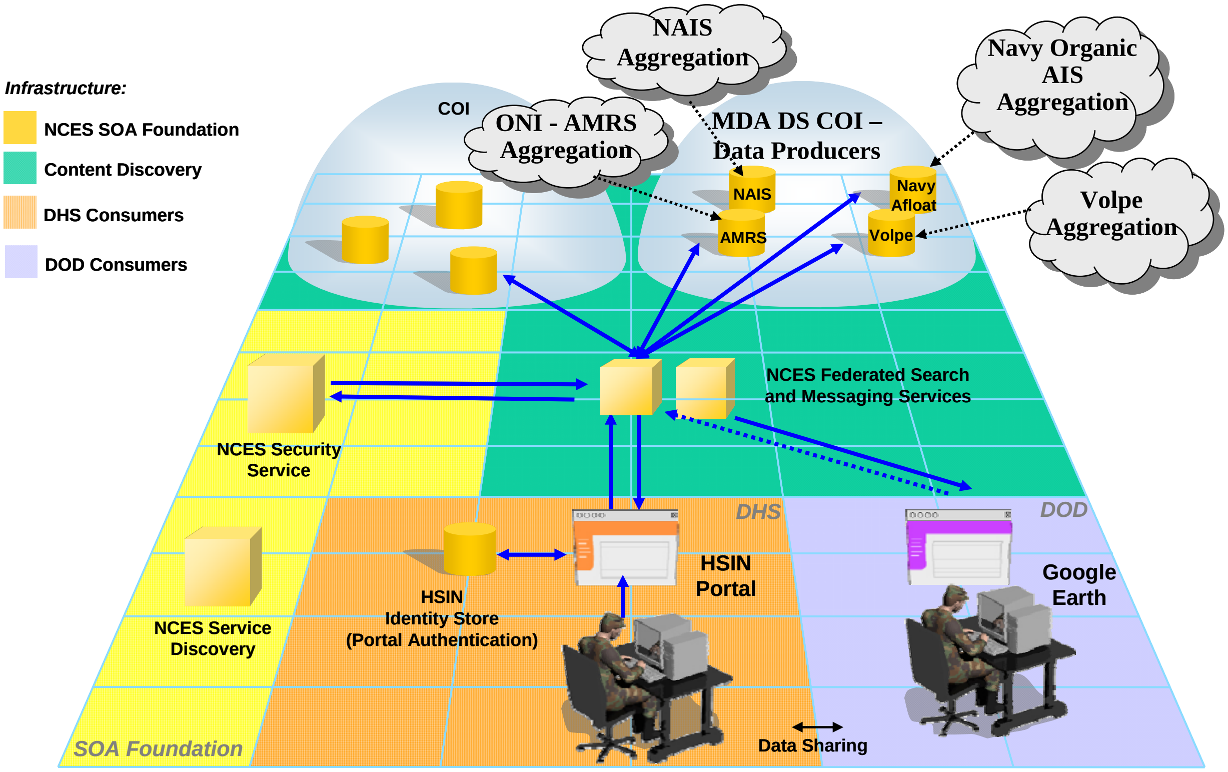


Figure 3. MDA DS COI Spiral 1 pilot high-level architecture.

In order to visualize the data, a link with the Space & Naval Warfare Systems Command (SPAWAR) Systems Center San Diego (SSC SD) AIS Aggregation Server was established using Google Earth. The COI developed the Google Maps Mediation Service (GMMS) to provide easy access and visibility of AIS data to COI consumers, including qualified but unanticipated consumers. GMMS is a tool that provides a UDOP for qualified users to access and view unclassified data in a controlled environment. User access is granted via a Common Access Card (CAC) or External Certification Authority (ECA) public key infrastructure (PKI) certification.

The Spiral 1 pilot project began in February 2006 and successfully demonstrated the capability to share unclassified AIS data using a common vocabulary and schema in October and December 2006. Its operational utility was assessed in an actual operations center (SeaHawk Charleston) during the Coalition Warrior Interoperability Demonstration (CWID) exercise in June 2007. CWID 2007 proved that the DHS HSIN and the NCES ECB could provide a net-centric method in an SOA environment to expose AIS data for publishing and subscription.

2.2.2 Spiral 2 Pilot Project

Having successfully demonstrated a net-centric data sharing capability in Spiral 1, the COI initiated the Spiral 2 pilot project to improve MDA schemas, expand the number of producers and consumers, develop additional value-added services, and prepare for transitioning the services to an operational capability. Common vocabularies and schemas not only facilitated universal understanding of AIS data, they also exposed opportunities for broader understanding of an expanded set of data. The COI expanded and enhanced the Spiral 1 information exchange schema for AIS to support the addition of new services planned for Spiral 2. The DMWG participated in the working groups for the Maritime Information Exchange Model (MIEM) and Universal Core (UCore) schemas. MIEM is a comprehensive schema designed to support expansion of the COI vocabulary to include a robust set of core data elements associated with vessel, cargo, people, and facilities. For Spiral 2, MIEM was used to develop schemas for one of the three value-added services: the Anomaly Detection Service (ADS). While we began working with UCore in this effort, the UCore standards were not ready in time to support Spiral 2 data delivery. It should be noted that UCore is an interagency information-sharing initiative intended to support multiple communities (i.e., DoD, DHS, Department of Justice (DOJ), and Intelligence Community (IC)). It is an information exchange specification and implementation profile that is a functional element of the National Strategy for Information Sharing. UCore will play a significant role in future MDA data sharing.

Spiral 2 also expanded the number of data producers and consumers to expose and share more MDA data and enrich the information environment. During spiral 2, the USCG expanded AIS coverage through the implementation of the USCG Nationwide AIS network. The USCG Research and Development Center (R&DC) operates the NAIS data publisher that shares the AIS vessel reports from the USCG NAIS network and from R&DC AIS efforts in long-range reception. The USCG AIS publisher prioritizes data for publishing, translates it to Extensible Markup Language (XML), and publishes it to the NCES Messaging Service. The USCG R&DC developed a Quality Assurance Consumer Node to connect to the NCES Messaging Service and retrieve MDA AIS messages. This consumer node parses the MDA AIS messages and stores the underlying AIS information. It also matches those incoming messages with messages sent from the NAIS Producer and records statistical information on receipt. A separate Web application, the Metric Analysis Tool (MAT), displays statistical information including status of the services, reliability, and latency metrics. These performance measurements were shared with the COI and has allowed the community to develop more reliable services. Additional producers and consumers include some who share information in a cross-domain environment, such as the Comprehensive Maritime Awareness (CMA) Joint

Concept Technology Demonstration (JCTD), Project SeaHawk, and Maritime Automated SuperTrack Enhanced Reporting (MASTER). They are demonstrating the ability to share information in a cross-domain environment, sharing unclassified AIS data in a classified environment and augmenting multiple sources of information to support operational analysis of elements of interest at the classified level.

The most widely known improvements on Spiral 1 include the addition of three value-added services: the Data Augmentation Service (DAS), the Historical Archive Service (HAS), and the ADS. The DAS leverages an authoritative reference data source to augment the AIS data being published to provide a richer information environment for the user. The HAS exposes existing AIS historical data archives via Web service and acts as a storefront access to historical AIS data. The ADS leverages the AIS data being published to provide a richer information environment for an existing anomaly detection system and then publishes any resulting anomalies to the NCES Messaging Service, which allows these discrepancies to be shared across the enterprise.

Finally, Spiral 2 data sharing services (which were successfully demonstrated to a senior DoD and DHS audience on 28 April 2008) was to transition services to an operational environment. As part of Spiral 1, the MDA DS COI created the GMMS and hosted it at SPAWAR Systems Center Pacific on a research and development network with access to the Non-Secure Internet Protocol Router Network (NIPRNET) and Internet. To transition this service into an operational environment, the MDA DS COI piloted a DoD Information Assurance Certification and Accreditation Process (DIACAP) that would allow all members of the MDA DS COI to honor and accept the certification and accreditation (C&A) of the GMMS without any additional service, department, or agency C&A testing. In addition, the MDA DS COI worked with DISA's Defense Enterprise Computing Centers (DECCs) to install GMMS at a hosted facility to provide the increased bandwidth, redundant communications links, scalability, and 24x7 support required for an operational service.

3 SPIRAL 3

Spirals 1 and 2 proved the concept of interagency information sharing across an enterprise network in an SOA environment. Focusing on AIS, those projects proved MDA could be enhanced through net-centric data sharing. However, the national vision for MDA includes representing data of all types and sources in a common operational picture that is accessible to anyone with valid needs and credentials. The ultimate intent is to have data available in any domain necessary to support the user and enhance MDA. Such architecture requires solutions for moving data between classified and unclassified domains as well as the necessary access controls to protect the data from unauthorized disclosure. For Spiral 3, the COI's next step was to expand the data sources to include sensitive data that cannot be openly shared without controlling accessibility. The goal was to implement a control mechanism that vetted potential consumers against the statutory and organizational requirements of data producers and demonstrate that sensitive data could be shared across an enterprise network without exposing it to unauthorized recipients.

The primary objectives of Spiral 3 included offering ANOA data as part of Web services on NCES, SILO data that exposes watch lists of vessels of interest (VOIs) in a common vocabulary that would be available on NIPRNET and the Secret Internet Protocol Router Network (SIPRNET), and an enhanced security framework using ABAC. ANOA and SILO were selected as the new data sources because of the sensitive nature of the information within. ANOA is based on the Coast Guard's statutory requirement for an NOA filed 96 hours prior to arriving in U.S. ports. It contains valuable information about the vessel, its cargo, and its crew, including PII, which cannot be shared outside the Coast Guard and law enforcement agencies.

SILO is an aggregated list of vessels of interest produced by the U.S. Navy's ONI. It includes classified as well as sensitive unclassified data about vessels posing a potential threat to the U.S. and is hosted on SIPRNET. ABAC was chosen as an enhanced security framework because it goes beyond requiring just a logon identification and password.

3.1 ABAC

ABAC is designed to measure known information about each individual attempting to access a site against required attributes. It is an industry approach to providing scalable access control at an enterprise level. ABAC is based on a trust-relationship among providers and consumers beyond system-to-system logon. It extends role-based credentials and seeks specific attributes such as citizenship, organization, association with law enforcement, etc. It measures digitally established attributes against policy decisions and enforcement to determine access to data. If a user accesses a Web service and requests access to data that requires protection, the request is vetted by policy to look for the necessary attributes before granting access. ABAC is scalable because two different users can access an information site and receive distinctly different sets of data, depending on their individual attributes. Some attributes equal some data; no attributes equal no data.

Access control for data sharing to date has been Role-based Access Control (RBAC). With RBAC, individuals log on to a system in an assigned role (i.e., user, administrator, etc.). If their logon credentials allow access to the site, they have access to any information on that site that does not require an additional logon. For Spirals 1 and 2, NCES' RBAC Security Services were used to enforce information-sharing restrictions determined by some of the data providers. Each subscriber was pre-defined by user type and pre-authorized to subscribe to the data. RBAC security services are still in use and will remain in place for the messaging services. RBAC has limited capability regarding the number of roles that can be defined and managed. A more flexible access control method that could be tailored to an individuals needs was desired. NOA also presents a sensitive data challenge not experienced in previous data sharing efforts. Coast Guard requirements, spelled out in the DHS *Handbook for Safeguarding Sensitive PII at DHS,* dictate that a policy is defined to establish need-to-know criteria that can be managed in an access control solution. SILO data presents a significant policy challenge to address aggregation of multi-source information, classification, cross-domain information transfer (NIPRNET/SIPRNET), and need to know.

3.1.1 Technical Approach for Implementing an ABAC Solution

RBAC would clearly not work for querying Spiral 3 data sets. Therefore, the initial approach to establishing an ABAC solution for ANOA had to include an enhanced security framework that offered certificate validation, searchable stores of attributes, policy administration, and policy decision. As planning continued and more options began to surface, the approach was expanded to offer more than one option. At the January 2008 COI Status Meeting, two possible solutions were presented:

- **Layer 7 Network Gateway:** Layer 7 Technologies created the SecureSpan XML Networking Gateway, referred to as the "Layer 7 Network Gateway" device. The COI saw it as an existing capability that can quickly filter out restricted fields and act as an attribute-based Policy Enforcement Point (PEP). The major drawback with the Layer 7 Network Gateway device is cost. At over $100K per unit and each Web service requiring a unit, cost would be prohibitive to a COI.

- **NCES Security Services:** Another possible solution was to use NCES Security Services. The source code is available and can be adapted to meet the COI's needs; the cost is much lower; and security is an established service rather than a hardware and software solution not yet developed. Nonetheless, it would require up-front time to adapt software to meet the requirements, many of which had not yet been determined. Furthermore, the use of NCES Security Services would not be controlled nor owned within the COI. Performance issues would need collaboration between the COI and DISA to resolve them, possibly taking inordinate amounts of time.

The PTWG's initial decision was to pursue NCES Security Services based on cost concerns. The intent was to modify the NCES Policy Decision Service (PDS) software to view attributes from a local Lightweight Directory Access Protocol (LDAP) database in addition to an external attribute store. Additionally, the services would provide a library to the Web services to filter data based on Security Assertion Markup Language (SAML) assertions provided by the NCES PDS. This solution would support traditional Web services but not publish/subscribe messaging. See Figure 4.

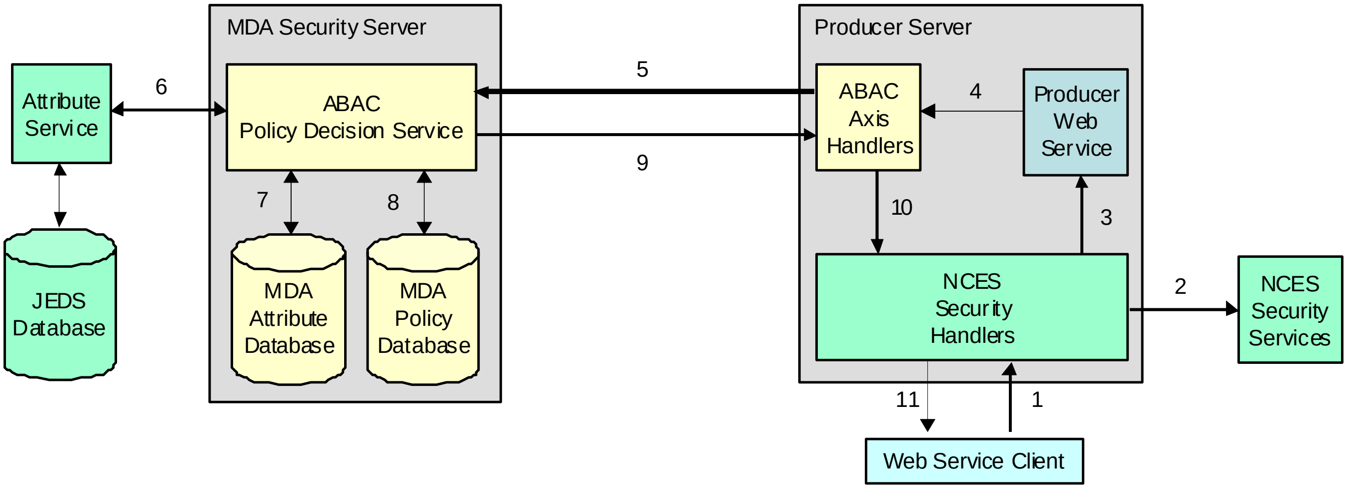


Figure 4. ABAC architecture, January 2008.

3.1.2 ABAC Governance

Prior to the Spiral 3 kickoff, the COI wanted to create a coalition of willing participants to share data across the enterprise. Recognizing that some data could not be shared without restrictions, the PTWG asked existing data providers to complete a policy framework that would identify what data could be shared, with whom it could be shared, what restrictions needed to be in place, and any data that could not be shared. The process needed to be iterative between data stewards and policy makers to ensure all data sharing scenarios were properly vetted against security policy. Respondents included Navy AIS, Volpe/Maritime Security Safety Information System (MSSIS), ONI Automated Merchant Reporting System (AMRS), USCG NAIS, USCG ANOA, and ONI SILO.

With a policy framework for ANOA data in place (see APPENDIX B), an ABAC solution was a reasonable expectation for Spiral 3. The Coast Guard ISR Data Analysis & Manipulation Division (CG-262) was firmly supportive of the effort, providing their plan for sharing ANOA data at the Spiral 3 Kickoff meeting in January 2008. For SILO, ONI had initially planned for SILO integration with ABAC as part of their Spiral 3 support. As their policy framework indicated (APPENDIX B), SILO data resides on SIPRNET, so a cross-domain solution (CDS) is required to transfer data to an unclassified domain. They planned to leverage an existing CDS to expose unclassified MDA data from the NIPRNET GMMS service to the SIPRNET. Once that was in place, ONI would then use the CDS to transition sanitized SILO data to the unclassified GMMS service through ABAC. As of the Spiral 3 demonstration on 31 March 2009, the certifications necessary to exercise the CDS from NIPRNET to SIPRNET had not yet been issued to ONI, so the first part of their plan could not be achieved. However, ABAC for SILO remains a goal for the future once the national security policy issues are resolved.

3.1.3 ABAC Architecture

Once it was clear that the NCES Security Services would not suffice as an ABAC solution, the PTWG proceeded with a design that built upon NCES's security but provided the granularity and scalability required for sensitive data. Access to specific resources (e.g., Web services, specific data, etc.) would be determined by user attributes such as citizenship, organization, association with law enforcement, etc. The prototype architecture was based on sharing ANOA data and is shown in Figure 5.

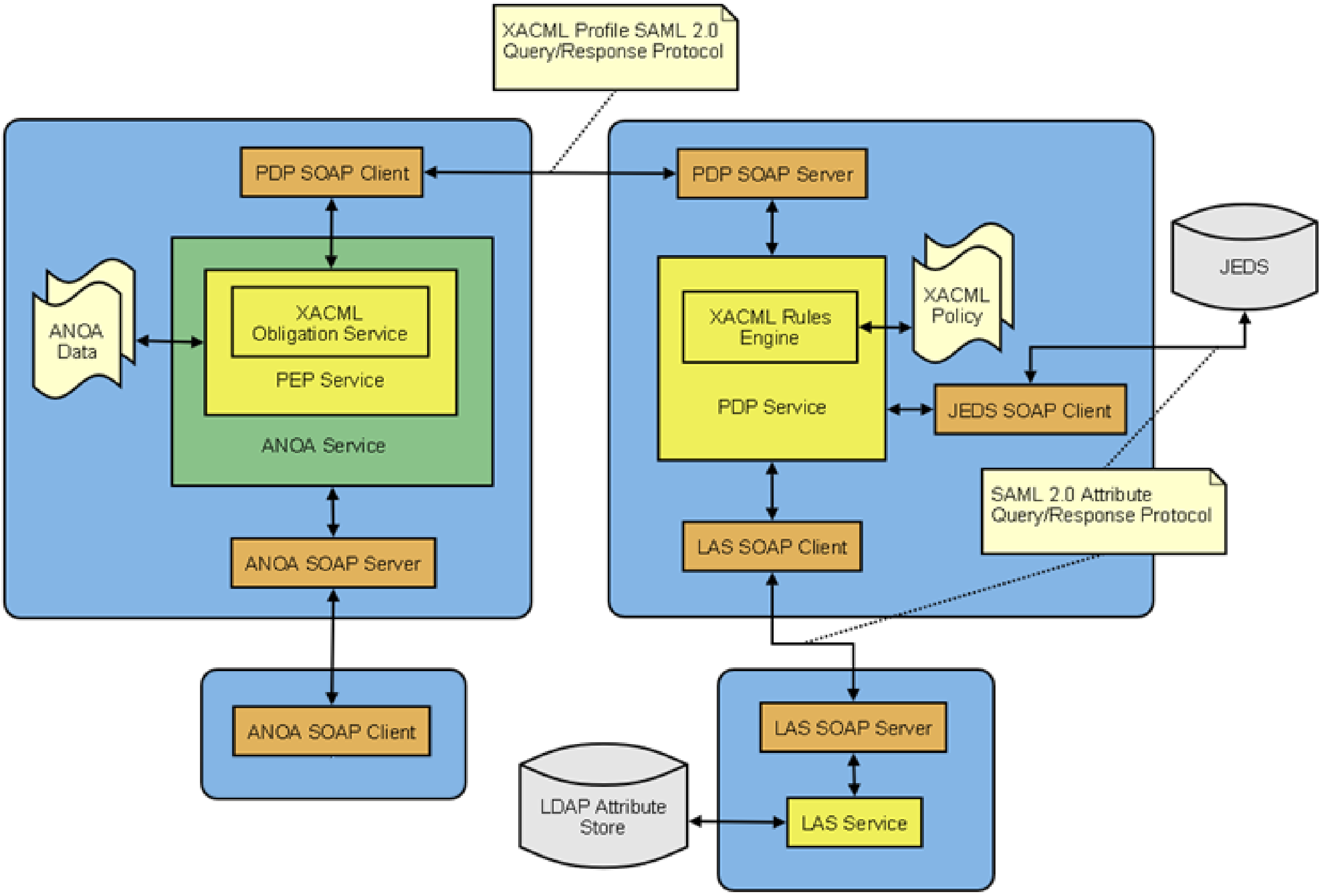


Figure 5. ANOA ABAC architecture, March 2009.

This design leverages industry standards to process requests for access to ANOA data. If a user attempts access, the request is processed through a Policy Enforcement Service (PES) using Extensible Access Control Markup Language (XACML), which in turn is processed through a PDS. The request is vetted against the Joint Enterprise Discovery Service (JEDS) (only for DoD users) and a Local Attribute Store (LAS) for the necessary attributes. SAML 2.0 is used to assess the attribute responses, and the user is granted access to the level of data dictated by the attributes returned. For access to ANOA data, there are three broad categories of user: U.S. MDA user, U.S. MDA and Law Enforcement user, and Non-U.S. (foreign) MDA user (see Figure 6).

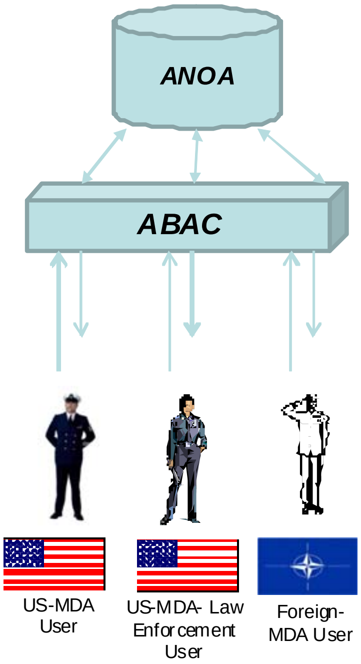


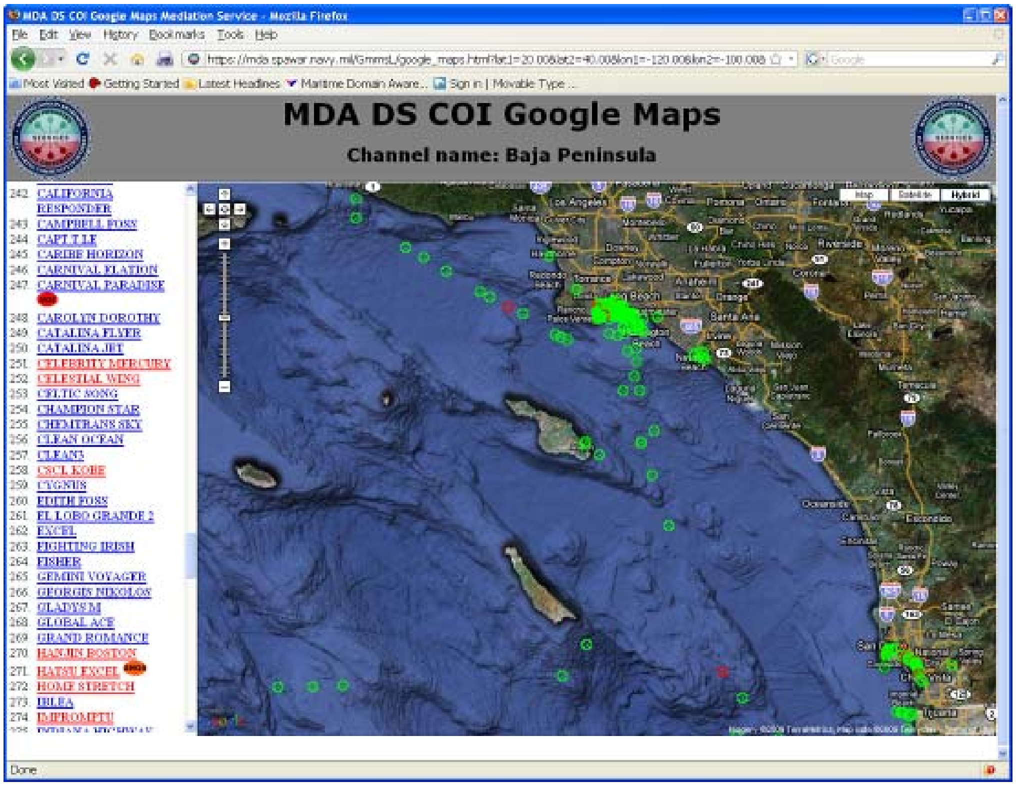
Figure 6. Users of ANOA data.

3.1.4 Data Access Through ABAC

Access to ANOA data through ABAC was successfully demonstrated during the Spiral 3 demonstration. Additionally, the Federated Search capability was also illustrated during that demonstration. The premise was that one of three different users would access ANOA data available on the GMMS in the same manner AIS data is accessed. Then, depending on the attributes of the user, different sets of data could be seen.

In the case of the foreign user, the vessel could be accessed but no ANOA data would be returned. For a U.S. MDA user, all ANOA data would be returned except the PII associated with crew and passengers. Law enforcement users would see *all* ANOA data, including the PII.

In the illustration in Figure 7, the vessel HATSU EXCEL displays a ANOA tag next to the name, demonstrating that the vessel has issued an ANOA. By selecting that vessel, the user can see specific information about the vessel, including location, ship's name, etc. In the next illustration (Figure 8), the user has the option to select the Advance Notice of Arrival Query, which will provide information about where the ship is headed, the expected time of arrival and departure, the last five ports visited, and other useful information.

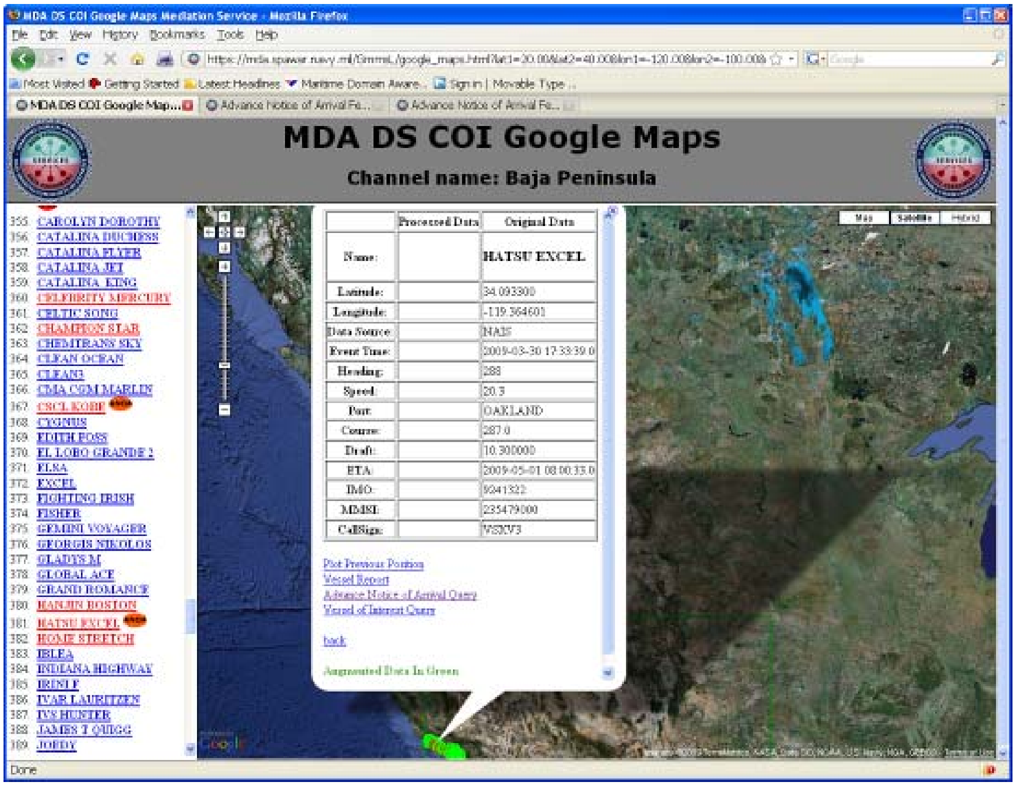

MDA DS COI Google Maps Mediation Service - Mozilla Firefox
File Edit View History Bookmarks Tools Help
https://mda.spawar.navy.mil/GmmsL/google_maps.html?lat1=20.00&lat2=40.00&lon1=-120.00&lon2=-100.00
Most Visited Getting Started Latest Headlines Maritime Domain Aware... Sign in | Movable Type ...
Map Satellite Hybrid
Los Angeles
Long Beach
Santa Ana
Done

MDA DS COI Google Maps

Channel name: Baja Peninsula

242 CALIFORNIA RESPONDER
243 CAMPBELL FOSS
244 CAPT T.LE
245 CARIBE HORIZON
246 CARNIVAL ELATION
247 CARNIVAL PARADISE
248 CAROLYN DOROTHY
249 CATALINA FLYER
250 CATALINA JET
251 CELEBRITY MERCURY
252 CELESTIAL WING
253 CELTIC SONG
254 CHAMPION STAR
255 CHEMTRANS SKY
256 CLEAN OCEAN
257 CLEAN3
258 CSCL KOBE
259 CYGNUS
260 EDITH FOSS
261 EL LOBO GRANDE 2
262 EXCEL
263 FIGHTING IRISH
264 FISHER
265 GEMINI VOYAGER
266 GEORGIS NIKOLOS
267 GLADYS M
268 GLOBAL ACE
269 GRAND ROMANCE
270 HANJIN BOSTON
271 HATSU EXCEL
272 HOME STRETCH
273 IBLEA
274 IMPROMPTU

Figure 7. Channel selected showing a vessel with an ANOA.


MDA DS COI Google Maps Mediation Service - Mozilla Firefox
File Edit View History Bookmarks Tools Help
https://mda.spawar.navy.mil/GmmsL/google_maps.html?lat1=20.00&lat2=40.00&lon1=-120.00&lon2=-100.00
Most Visited Getting Started Latest Headlines Maritime Domain Aware... Sign in | Movable Type ...
MDA DS COI Google Map...
Advance Notice of Arrival Fe...
Advance Notice of Arrival Fe...
Map Satellite Hybrid
Done

MDA DS COI Google Maps

Channel name: Baja Peninsula

355 CAROLYN DOROTHY
356 CATALINA DUCHESS
357 CATALINA FLYER
358 CATALINA JET
359 CATALINA KING
360 CELEBRITY MERCURY
361 CELTIC SONG
362 CHAMPION STAR
363 CHEMTRANS SKY
364 CLEAN OCEAN
365 CLEAN3
366 CMA CGM MARLIN
367 CSCL KOBE
368 CYGNUS
369 EDITH FOSS
370 EL LOBO GRANDE 2
371 ELSA
372 EXCEL
373 FIGHTING IRISH
374 FISHER
375 GEMINI VOYAGER
376 GEORGIS NIKOLOS
377 GLADYS M
378 GLOBAL ACE
379 GRAND ROMANCE
380 HANJIN BOSTON
381 HATSU EXCEL
382 HOME STRETCH
383 IBLEA
384 INDIANA HIGHWAY
385 IRINI F
386 IVAR LAURITZEN
387 IVS HUNTER
388 JAMES T QUIGG
389 JOEDY

	Processed Data	Original Data
Name:		HATSU EXCEL
Latitude:		34.093300
Longitude:		-119.364601
Data Source:		NAIS
Event Time:		2009-03-30 17:33:39.0
Heading:		288
Speed:		20.3
Port:		OAKLAND
Course:		287.0
Draft:		10.300000
ETA:		2009-05-01 08:00:33.0
IMO:		9041322
MMSI:		235479000
CallSign:		VSKV3

Plot Previous Position
Vessel Report
Advance Notice of Arrival Query
Vessel of Interest Query

back

Augmented Data In Green

Figure 8. Basic vessel information with link to Advance Notice of Arrival Query.

3.2 ANOA

ANOA data is the information contained in the Coast Guard's NOA, which all U.S. and foreign vessels bound for or departing from ports or places in the U.S. must file at least 96 hours in advance (see APPENDIX C). The 96-hour requirement, implemented as a Federal regulation after the attacks of September 11, 2001, changed what had been a 24-hour requirement and gives ports and operations centers more time to analyze a vessel, its cargo, and the people aboard to properly determine potential threats. As such, ANOA data is predictive information triggering analysis of a vessel well in advance of its arrival in a U.S. port. It provides detailed information about the vessel, the voyage (origination, destinations, etc.), the cargo, and the intended date/time of departure. It also includes specific PII about each crew member and any passengers who may be onboard. The PII makes ANOA data sensitive and subject to statutory restrictions on sharing it outside the Coast Guard and law enforcement entities.

After final preparations, publishing of ANOA data (without PII) began on February 15, 2009. As of the writing of this report, it continues to be published directly from MAGNet to OSC using the Enterprise Service Bus (ESB), and on to the NCES Messaging Service (ECB). It is published in the SANS schema in 1-hour intervals to GMMS in five geographic channels, established specifically for ANOA, based on port of arrival. Access control is managed by the PTWG using NCES-provided RBAC. Federated search queries are also possible by ANOA Identification (ID), Captain of the Port, IMO, vessel name, or vessel call sign. Full ANOA data with PII in accordance with the restrictions outlined in the Data Sharing Policy Framework requires the implementation of the ABAC.

3.2.1 Technical Approach for Sharing ANOA Data

NOA data is collected at the National Vessel Movement Center (NVMC) in Kearneysville, WV and entered into the Ship Arrival Notification System (SANS) database. It is then replicated into the Maritime Awareness Global Network (MAGNet) database for distribution to MAGNet consumers. For Spiral 3, the PTWG established a relationship with the MAGNet Program Office (CG-262) to determine a methodology for exposing non-sensitive NOA data to the COI using NCES' messaging and Federated Search capabilities. MAGNet had been working on a data sharing plan since the Spiral 3 project was approved and briefed it at the Kickoff meeting in January 2008. The initial plan was to begin publishing ANOA data from the R&DC to NCES in March 2008. It included publishing all ANOA data, with the exception of PII, at least hourly to geographic channels displayed on GMMS, based on the port of arrival. Initial development was to take place using the NCES ECB, with a transition to the NCES Managed Services Platform (MSP) once it was deployed by DISA. The MSP was due to have more robust capabilities than the ECB, which would presumably translate to better messaging and Federated Search capabilities.

MIEM was chosen as the schema for ANOA data sharing based on its use with other MDA-related data sets. In addition to publishing to GMMS, MAGNet planned to enable a query service for ANOA via the NCES Federated Search Service, similar to the Historical Archive Service demonstrated in Spiral 2. Access to the GMMS data would be controlled by the PTWG, and protection of the PII would be controlled within the Coast Guard.

To guard against unintended disclosure of ANOA data (including PII) CG-262 planned to only publish simulated data to prove the process worked. Consumers would be able to access GMMS and visualize simulated ANOA data in the same manner they did AIS data. Federated searches by port and vessel would also be available, but PII would not be accessible in any form until an acceptable access control method was implemented. The following timeline was established to implement the strategy for sharing ANOA data.

- June 2008: The MIEM schema extension would be complete for ANOA data
- July 2008: Ports of arrival would be mapped to GMMS channels for display
- Aug 2008: Initial Operational Test & Evaluation (IOT&E) for NCES MSP would be conducted
- September 2008: ANOA data without PII would be published
- September 2008: U.S. Coast Guard (CG-26) would sign off on PII Policy
- October 2008: ANOA data without PII would be available for Federated Search
- October 2008: ANOA data with PII would be available for publishing
- January 2009: ANOA data with PII would be available for Federated Search
- January 2009: All functionality installed and available
- March 2009: Spiral 3 Demonstration

This approach would prove challenging for many reasons. There were governance and policy issues, problems with NCES services, and schema compatibility problems, all of which would affect the final implementation.

3.2.2 ANOA Governance

The requirement to protect PII from unauthorized disclosure is governed by law and regulation. The Coast Guard is governed by the DHS *Handbook for Safeguarding Sensitive PII at DHS*, and CG-26 is responsible for ensuring those requirements are met. CG-262 is specifically responsible for PII associated with ANOA data. Access to ANOA data is normally controlled via point-to-point connections that were easily governed between organizations using Memoranda of Understanding (MOUs). For Spiral 3, they would undergo a paradigm shift from one-to-one agreements to centralized control that required trusting technology to interpret and enforce policy. CG-262 saw the potential benefits of this new approach had committed to the concept in full support of Spiral 3. The Data Sharing Policy Framework (APPENDIX B) was completed to illustrate that PII data was restricted to certain users, but the rest of ANOA data could be shared with users authorized to access the Web service.

Throughout the course of the project, MAGNet team (CG262 and OSC) worked closely with the Emerging Technologies Team (ETT) at the Operations Systems Center (OSC) in Martinsburg, WV and the Coast Guard R&DC in New London, CT to create the best process by which ANOA data could be shared as agreed with the COI. No PII would be published initially, but plans for full ANOA were in place, ready to execute once ABAC was implemented. As the project proceeded, the plan evolved to publishing ANOA data from MAGNet to the CG Enterprise Service Bus (ESB) at OSC , who in turn would publish it to NCES. Regular bi-weekly teleconferences among R&DC, ETT, and MAGNet were held throughout the project to keep the plan moving forward. It should be noted that this single effort also provided NOA data to other Coast Guard Projects via the ESB, specifically the Long Range Identification and Tracking (LRIT) and Interagency Operation Centers (IOC/C21) development effort. Close interaction with the data steward throughout the development was critical to deliver a technical solution that met CG-26 policy requirements.

3.2.3 NCES Transition and ANOA

While the Coast Guard team was working on an ANOA solution DISA was continuing with their plans to transition their NCES messaging services from the ECB to the MSP. The COI continued to support the transition as an early adopter with the expectation that services would improve significantly. COI members underwent training to connect, or “onboard” to the MSP, and the PTWG expended significant effort and time preparing to publish MIEM-formatted ANOA data to the MSP. As of September 2008, the IOT&E date had come and gone with no transition. The PTWG made attempts to publish to the MSP with no success.

DISA was confident enough in their schedule that they tentatively planned to terminate the ECB, forcing users to begin to switch to the MSP. Consumers had begun training for the shift and discussions between the PTWG and DISA regarding the transition were ongoing throughout the Fall of 2008. While the ECB was functional, it was not designed to process the ever-growing amount of AIS data, or the amount of additional ANOA data dictated by Spiral 3. It was also not designed to meet the requirement for guaranteed delivery. Deployment of the MSP was to solve most if not all of the issues with the ECB. However, despite continued plans for a spring-time deployment, DISA eventually declared a work-stoppage on MSP development, and it became clear that messaging and other NCES services would continue on the ECB.

The Navy and Coast Guard had expended a great deal of effort in anticipation of the MSP that might have otherwise been productive toward an ECB-based solution. Nonetheless, solutions regarding publishing ANOA data to the NCES messaging service were delayed, as were the Federated Search capabilities. As a result of several meetings with the PTWG, DISA has been helpful is solving some of the issues, but until the ECB is upgraded with some of the features advertised with the MSP, data sharing through NCES will continue to be problematic. DISA plans to roll out the ECB upgrades in mid-summer 2009, and the RDC will continue to monitor their progress.

3.2.4 ANOA Schema

Because MIEM was gaining acceptance as a standard among data providers, MAGNet began using MIEM 0.8 as an Alpha test case for ANOA in preparation for Spiral 3. However, it proved to be problematic due to complexities in understandability and readability. Some of the issues were corrected in MIEM 0.9, the Beta version, and it was thus chosen as the schema for the Spiral 3 ANOA service. Development of the MIEM solution continued throughout most of 2008, completing the XML translation in November. However, problems persisted in the implementation. Specifically, the MIEM is more stringent than the SANS format, so it did not support translation of all the ANOA data elements. For instance, because port name identification requires a unique value in MIEM, port names from SANS will not translate directly. This occurs because port names are often spelled differently from one vessel to another. There is no way to translate spelling variables into unique values in MIEM. As it became clear that MIEM was unwieldy and ineffective for ANOA data translation, the MAGNet team had to rework the solution to achieve ANOA publishing and search services with the time and resources available. In December 2008, the decision was made to forego MIEM 0.9 in favor of the simpler Coast Guard SANS schema. For more information on architectures and schemas associated with Spiral 3, see APPENDIX D.

As of February 15th 2009, ANOA data is published in the SANS format and satisfies the understandability and readability requirements that were not fulfilled by MIEM. However, MIEM is undergoing changes and will transition into the maritime domain extensions of the National Information Exchange Model (NIEM). NIEM use is required by DHS under many grant programs and will likely be required by DHS for future interagency data sharing solutions. To provide feedback on the quality of ANOA data publishing, throughput metrics will be collected at the Coast Guard R&DC to measure both the publishing process and the consumption process. APPENDIX E describes MAT as well as the other services provided in the data sharing process.

3.2.5 ANOA Architecture

The Coast Guard team working in conjunction with the PTWG developed the ANOA architecture over the course of the development. The final architecture evolved to meet the requirements of the CG-262 and OSC while delivering ANOA for the MDA DS COI. The ANOA architecture (Figure 9) indicates the users connecting from Local Systems through NCES Messaging to subscribe to ANOA published messages. The USCG OSC ETT publishes data directly to the NCES Messaging bus in hourly intervals. This data is then delivered to all subscribed consumers. An unanticipated user will be able to access the same data by using the NCES Federated Search Aggregator to perform queries against multiple data sources including the USCG OSC NOA data.

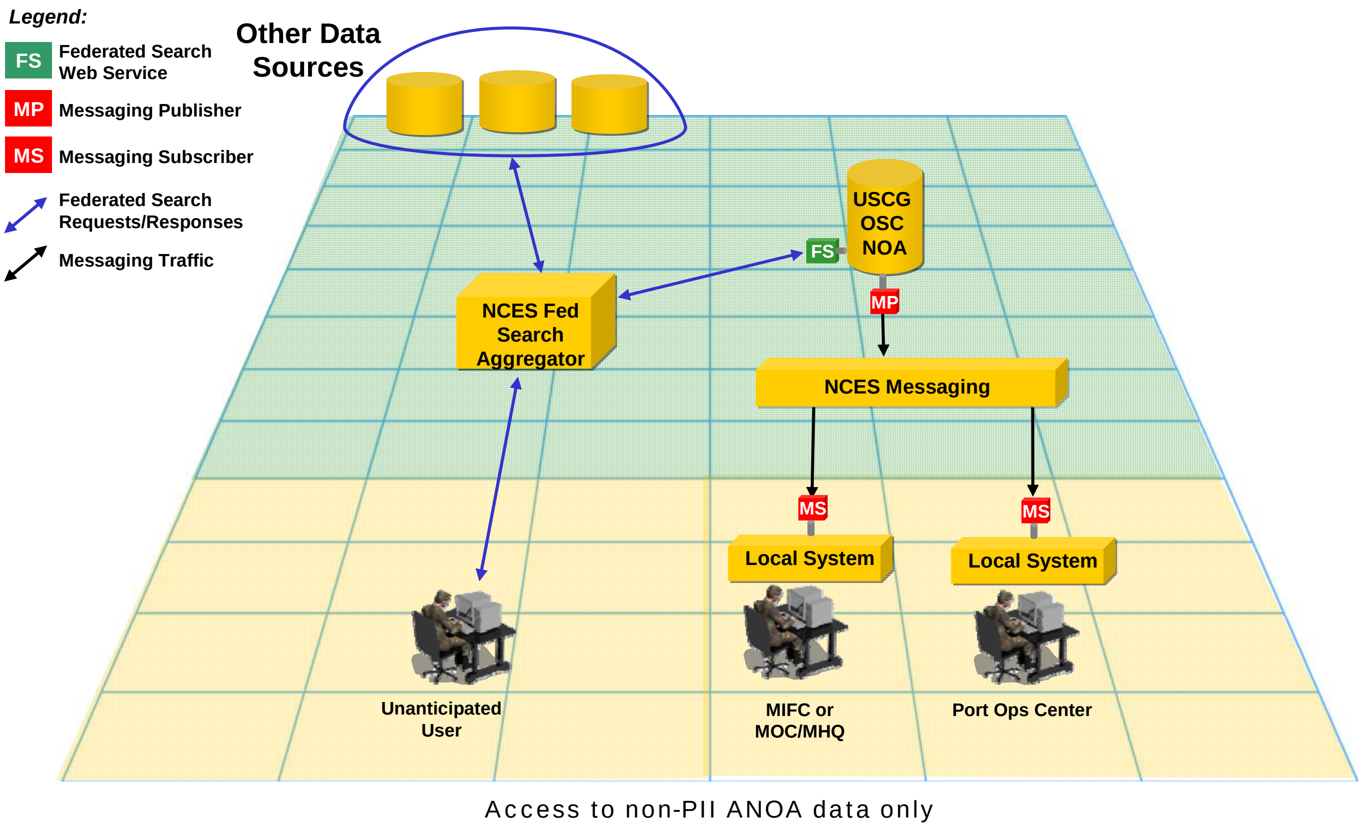
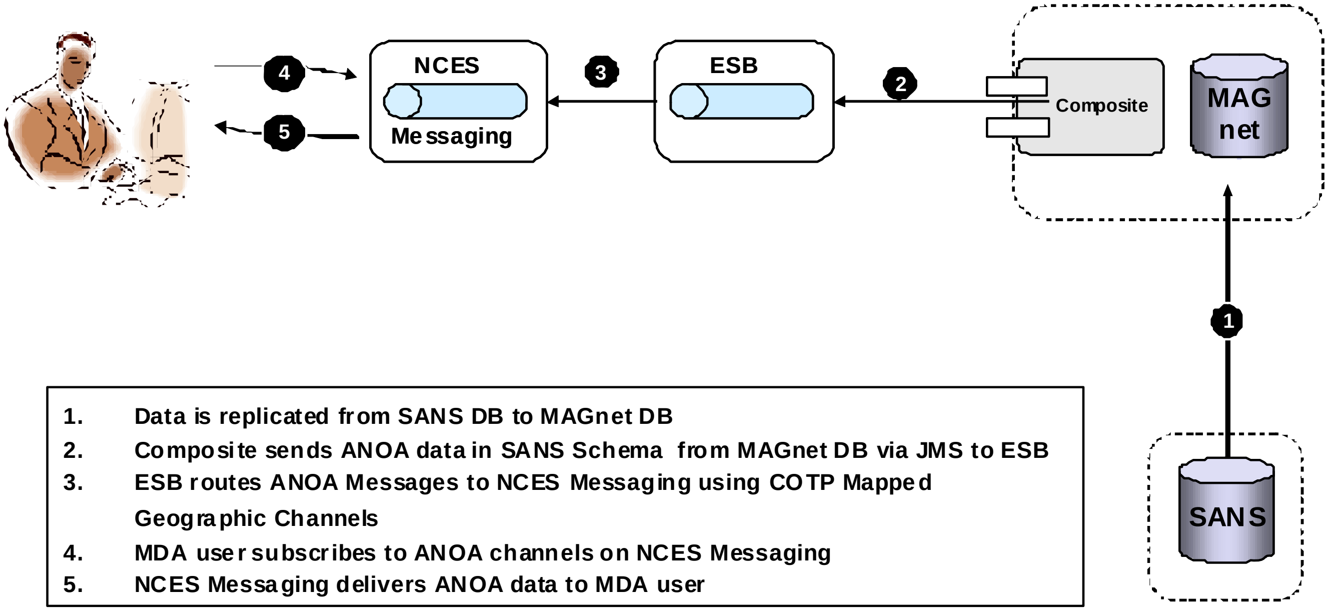


Figure 9. ANOA architecture.

3.2.5.1 ANOA Publishing Architecture

Figure 10 shows how data is replicated from the SANS database to MAGNet and then published out to NCES Messaging through the OSC ESB.



1. Data is replicated from SANS DB to MAGnet DB
2. Composite sends ANOA data in SANS Schema from MAGnet DB via JMS to ESB
3. ESB routes ANOA Messages to NCES Messaging using COTP Mapped Geographic Channels
4. MDA user subscribes to ANOA channels on NCES Messaging
5. NCES Messaging delivers ANOA data to MDA user

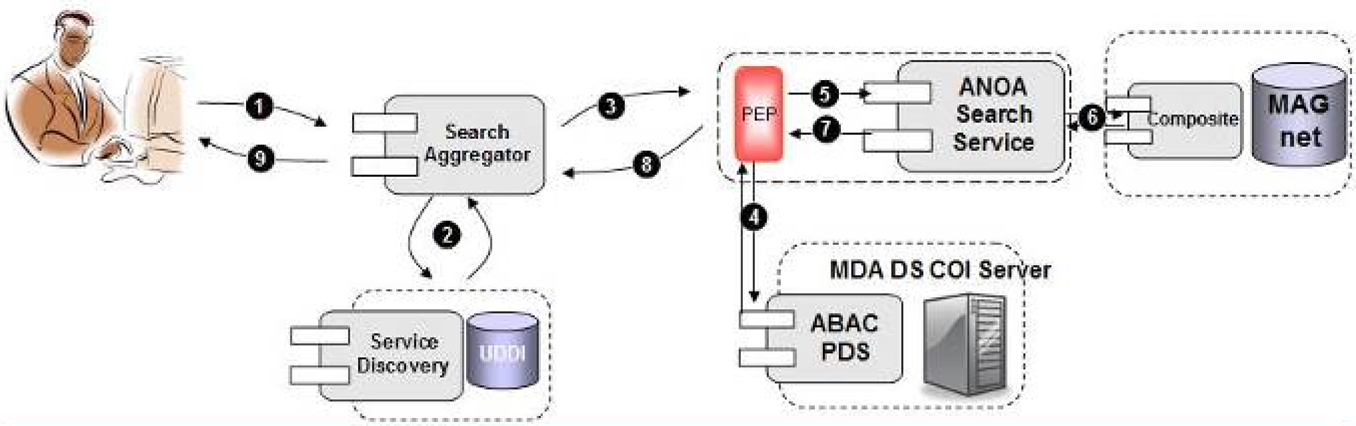
Figure 10. ANOA publishing architecture.

3.2.5.2 ANOA Federated Search Architecture

The ANOA Federated Search architecture (Figure 11) shows the consumer request to NCES Federated Search Aggregator which in turn sends requests to the ANOA Search Service through universal description, discovery and integration (UDDI) lookup in the NCES Service Discovery. The ANOA Search Service would forward the request against the MAGNet Composite data service and retrieve the results. The architecture also indicates a PEP that would enforce policy decisions based on user credentials against the proposed ABAC solution. The sanitized response is returned back to the consumer through the Search Aggregator.

3.3 SILO

SILO is part of the Global Maritime Intelligence Integration (GMII) Plan, which directs DoD and DHS to make use of legacy intelligence capabilities, existing policies, and operational relationships to integrate all available data, information, and intelligence to support maritime security planning and operations. It is an integrated list of vessels that have been identified by various sources within DoD and DHS as “vessels of interest.” Several operational and intelligence organizations maintain lists of vessels to “look out” for, keeping track of where the vessel goes, what cargo the vessel carries, and who in the crew or passenger list may be of interest. These lists are consolidated by ONI and integrated into a single lookout list, thus the name Single Integrated LookOut. SILO is intended to provide access to a single source of all vessels of domestic and global intelligence interest in coordination with cognizant authorities and operational centers. It will offer greater awareness of specific VOIs from an integrated view. Because the information is highly sensitive and usually classified, the prospect of sharing it in an unclassified environment presents major challenges.



1. Consumer makes discovery request
2. Search Aggregator queries Service Discovery for relevant Search Services
3. Search Aggregator distributes request to relevant Search Services (ANOA Search Service)
4. Web Service requests are intercepted by the PEP and forwarded to the ABAC PDS for a policy decision for authentication and authorization to each data element.
5. Calls are routed to the ANOA Search Service.
6. ANOA Search Service process the call and returns data from data sources.
7. Based on policy decisions the PEP strips out any restricted data elements.
8. The sanitized response is sent to the search aggregator.
9. Search Aggregator returns all search results to the consumer.

Figure 11. ANOA Federated Search architecture.

The guiding philosophy of the COI is to provide information access and integration to COI member organizations, plus unanticipated consumers with legitimate qualifications and a valid need for the information. ONI and Coast Guard are responsible as co-leads for implementing a SILO data sharing solution that improves situational awareness using standardized exchange formats and vocabularies. As such, ONI completed a Data Sharing Policy Framework identifying the restrictions for sharing SILO data on an unclassified network (see APPENDIX B).

3.3.1 Technical Approach for Sharing SILO Data

As of January 2008, SILO existed as a proof-of-concept on SIPRNET under Phase 1 of SILO development. It is intended to provide a standardized VOI exchange format and, in the future, a VOI lexicon. In Phase 1, SILO aggregated data from willing participants (e.g., ONI, Coast Guard) into a single VOI list. It used an interface for browsing, sorting, and searching vessel lookouts. It had the capability to export data to multiple formats (i.e., Atom, really simple syndication (RSS) , geographic RSS (GeoRSS), Keyhole Markup Language (KML), comma separated value (CSV), JavaScript Object Notation (JSON), text, and HyperText Markup Language (HTML)). It also incorporated links back to the original point of contact and websites for additional information. Its greatest limitation was that it ran inside the ONI firewall on SIPRNET. There was no need for access control because anyone authorized to access SIPRNET already had the right attributes.

For Phase 2, the intent was to define operational concerns, refine user interfaces, and increase the number of list providers. MIEM was to be added as an export schema. The main goal for Phase 2 was to complete development by April 2008 and deploy it to the ONI portal by June 2008.

Another critical goal of Phase 2 SILO was to integrate with the MDA DS COI efforts to standardize schema, vocabularies, and publishing strategies. COI integration was to assist in the following objectives:

- Extending MIEM support to importing data as well as exporting it
- Publishing on NCES in 4-hour blocks
  - Would publish to the ECB initially, then transition to the MSP
  - Publishing to the NIPRNET requires support from DISCA IA32 for the CDS
- Providing Federated Search capabilities to allow queries of VOIs
- Integrating with the ABAC solution for restricted data

Phase 3 commenced in July 2008 with the goal of publishing to the NCES on SIPRNET and eventually on the NIPRNET. Phase 3 SILO was in full support of Spiral 3 goals, including identifying a channel structure (GMMS) and obtaining server certifications for both NIPRNET and SIPRNET.

In Phase 3, the COI (ONI) planned to begin publishing SILO to SIPRNET using NCES ECB as early as August 2008, and a Federated Search capability for SIPRNET was to be in place in October 2008.

3.3.2 SILO Governance

Because even unclassified VOI data is highly sensitive, most stewards of lookout lists resisted consolidation and publishing to open source technology. However, the National Strategy for Data Sharing specifically addresses making information of intelligence value available to as many organizations as possible, using net-centric options to populate the COP. Recognizing the necessity of shared data, ONI began SILO Phase 1 in 2007, developing requirements and defining Atom standards for publishing/subscribing VOI data. In 2008, SILO executed its Phase 2 strategy with the following accomplishments:

- Visited multiple sites to solicit their support in publishing VOI lists to SILO.
- Developed aggregate lists from ONI, Maritime Intelligence Fusion Center Atlantic (MIFCLANT), USCG CoastWatch, and Maritime Intelligence Fusion Center Pacific (MIFCPAC).
- Deployed proof of concept on SIPRNET.
- Established the capability to sort, filter, and search.
- Exported data in a variety of formats (CSV, MIEM, RSS, Atom, over-the-horizon (OTH)-Gold, text).
- Assisted with SILO version of MIEM specification.
- Created security markings based on information security marking (ISM) XML specifications.
- Integrated Fusion Map based on National Geospatial-Intelligence Agency (NGA) Web.

For 2009, SILO Phase 3 supported the MDA DS COI Spiral 3 Demonstration in March. Although valid SILO data was restricted to SIPRNET, “dummy” or example data was provided for inclusion in the demonstration. The PTWG was able to illustrate how VOI data can be accessed in GMMS on SIPRNET, and how it would look on NIPRNET as well. Furthermore, the PTWG was able to demonstrate the Federated Search process for SILO, again using example data. Despite that lack of real-time, valid data, the COI proved the value of the ability to share sensitive data in a net-centric environment.

3.3.3 SILO Architecture

The architecture for Phase 1 SILO enabled vessel list producers (e.g., ONI, MIFCLANT/MIFCPAC, etc.) to aggregate their lists into one, and publish it to SILO Web services. From there, they successfully exported the data in a variety of formats that allowed for different access configurations. Data could be published directly into an Atom reader, or to other applications or portals. See Figure 12.

In Phase 2, ONI was able to increase the number of list providers and achieved buy-in to sharing the data in a net-centric environment, so long as it was on SIPRNET. No solution was available for sharing SILO data on NIPRNET during Phase 2. In July 2008 Phase 3 (v) 2.0 was implemented with new capabilities.

- New user interface features were added:
  - Paging, configurable columns, movable windows, search by columns, auto-complete
- MDA NCES publishing
  - All vessels over SILO channel (SIPRNET) in SILO-MIEM format every 4 hours
  - Still waiting on SIPRNET PKI server certificate for transfer of NIPRNET data to SIPRNET
- MDA Federated Search
  - Web Service to search for ship returning SILO-MIEM
- Deployment
  - Dummy data provided in support of the MDA DS COI Spiral 3 demonstration on NIPRNET
  - Valid SILO data published on SIPRNET

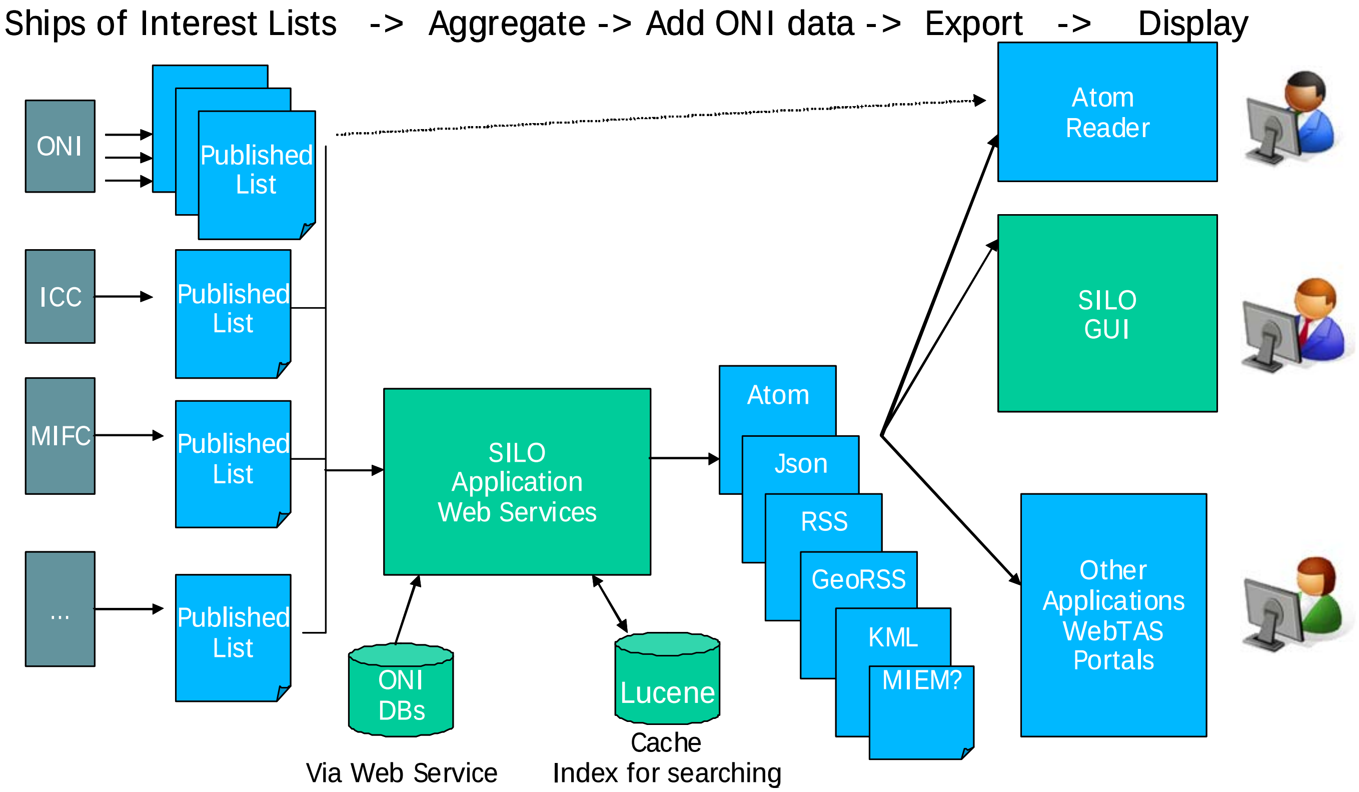


Figure 12. Phase 1 SILO architecture.

3.3.4 Cross-domain Solution

Classified information must be protected against inadvertent placement on unclassified domains. There are prohibitions against classified and unclassified networks being connected. However, there are times when NIPRNET information would be useful on SIPRNET as well. The only way to make that possible is to create a cross-domain process that allows that transfer but ensures inadvertent compromises do not take place. Prior to Spiral 3, the MDA DS COI had received requests from potential consumers of AIS data to receive the data on SIPRNET, which would require a cross-domain solution. DISA had already done some cross-domain work for other customers, so the COI leveraged that experience and engaged in discussions with DISA IA32 and the National Security Agency (NSA), the authorities for sharing data across domains (i.e., unclassified-to-classified, etc.). The goal was to establish the necessary certification and accreditation for a CDS enabling NIPRNET-to-SIPRNET transfer of AIS data. DISA IA32 was highly interested in using the MDA DS COI as a test case for this capability, so they began coordination with NSA in February 2008 to review C&A documentation, architecture, data flows, security posture, threats, controls, etc. and to perform pre-certification test and evaluation (CT&E) testing.

DISA briefed the Defense Intelligence Agency (IA)/Security Accreditation Working Group and received an Interim Authority To Operate (IATO) to support the MDA DS COI and TW08 on 13 May 2008.

The Cross Domain Web Services Gateway (CDWSG) utilizes existing trusted guard devices wrapped with XML firewalls and proxy technologies to provide for the bi-directional exchange of pre-authorized Web service transactions across security enclave boundaries. The CDWSG supports cross-domain transfer of information as follows:

- The low side of the CDWSG receives messages published from the MDA DS COI Publishing Agent.
- Connections to the CDWSG are established using two-way Secure Sockets Layer (SSL), and the MDA DS COI Publishing Agent uses an authorized PKI certificate to connect to the CDWSG.
- The XML firewall within the CDWSG will verify that each message is well formed, complies with the MDA DS COI XML schemas, and is digitally signed.
- The DSG receives each message and re-validates it against the combined MDA DS COI XML schema.
- If the DSG validation is successful, the message is delivered to the high side of the CDWSG.

The plan to share AIS data from NIPRNET to SIPRNET was possible through the CDWSG. The Solers Pilot Technical Team (PTT) developed an MDA Publishing Agent that subscribes to the MDA DS COI channels on the NIPR NCES Messaging Service. It requires the use of an authorized PKI Certificate, and NCES is configured to allow subscription to all MDA channels. During support for TW08, the MDA DS COI enhanced the MDA Publishing Agent to support schema validation, add data mediation, and support integration testing with the DISA IA32 CDWSG team.

For Phase 3 (v) 3.0, ONI is awaiting PKI certificates to subscribe to NIPRNET data for publishing to SIPRNET. Plans continue for development of a CDS for SIPRNET-to-NIPRNET publishing, but innovative applications of policy and technology must take place before that is possible.

3.4 Spiral 3 Demonstration

A demonstration of Spiral 3 capabilities was conducted on 31 March 2009 at the DISA Skyline 7 facility to an audience of flag-level officers and senior executive civilians. There were representatives from the COI, producer and consumer organizations, as well as other organizations interested in the future of data sharing. The presentation consisted of a brief background of the COI, a recap of Spirals 1 and 2, and the goals and expectations from Spiral 3. A thorough presentation of information on ANOA and SILO data was given, along with an in-depth description of ABAC and why it is necessary for data sharing. The capabilities demonstration consisted of a flash presentation depicting the sequence of events and information flow when data is sent from a producer to a consumer, and how a consumer is able to query the system for information. (See Figure 13.)

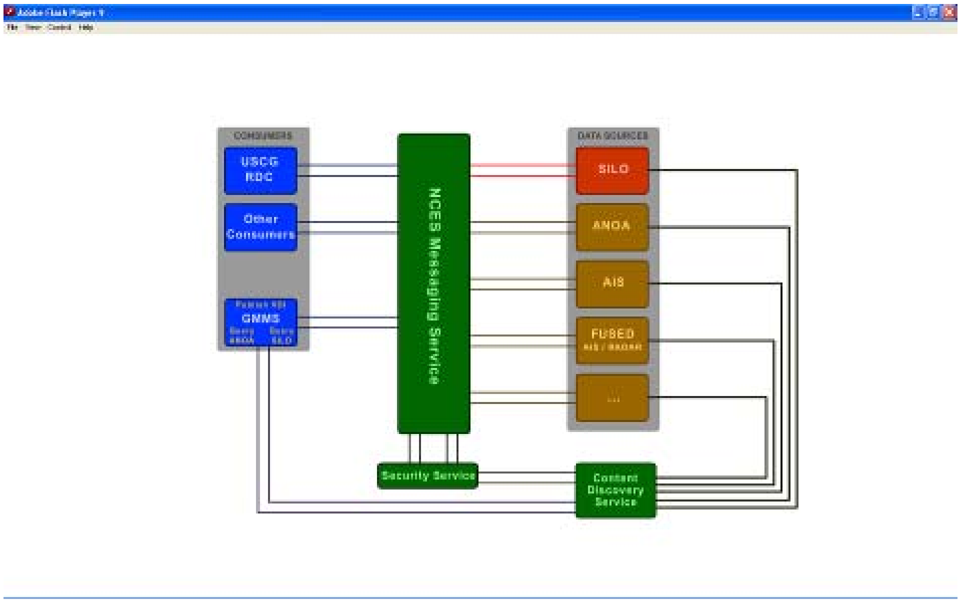
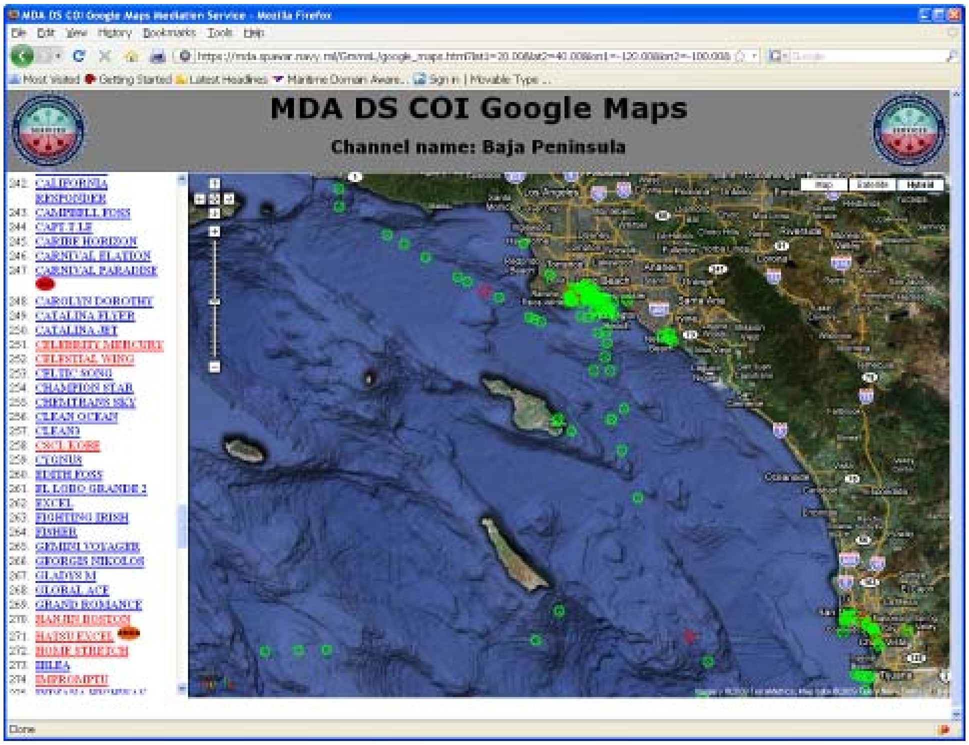


Figure 13. Data flow through NCES.

Figure 14 through Figure 17 illustrate what consumers would see when accessing the GMMS with ANOA and SILO information available. Vessels with ANOA information available are tagged with an orange "ANOA" tag, while vessels with SILO data available are tagged with a red "VOI" tag. Figure 14 depicts the Baja Peninsula Channel in GMMS, and the list of vessels on the left illustrates a ship with an ANOA tag on it (HATSU EXCEL), indicating a Notice of Arrival is available for this ship.


MDA DS COI Google Maps Mediation Service - Mozilla Firefox
File Edit View History Bookmarks Tools Help
Most Visited
Getting Started
Latest Headlines
Maritime Domain Aware...
Sign in | Movable Type ...
MDA DS COI Google Maps
Channel name: Baja Peninsula
Map
Satellite
Hybrid
Los Angeles
Done

242. CALIFORNIA RESPONDER
243. CAMPBELL FOSS
244. CAPT T LE
245. CARIBE HORIZON
246. CARNIVAL ELATION
247. CARNIVAL PARADISE
248. CAROLYN DOROTHY
249. CATALINA FLYER
250. CATALINA JET
251. CELEBRITY MERCURY
252. CELESTIAL WING
253. CELTIC SONG
254. CHAMPION STAR
255. CHEMTRANS SKY
256. CLEAN OCEAN
257. CLEANS
258. CSCL KOBE
259. CYGNUS
260. EDITH FOSS
261. EL LOBO GRANDE 2
262. EXCEL
263. FIGHTING IRISH
264. FISHER
265. GEMINI VOYAGER
266. GEORGES NIKOLOS
267. GLADYS M
268. GLOBAL ACE
269. GRAND ROMANCE
270. HANJIN BOSTON
271. HATSU EXCEL
272. HOME STRETCH
273. HILEA
274. IMPROMPTU

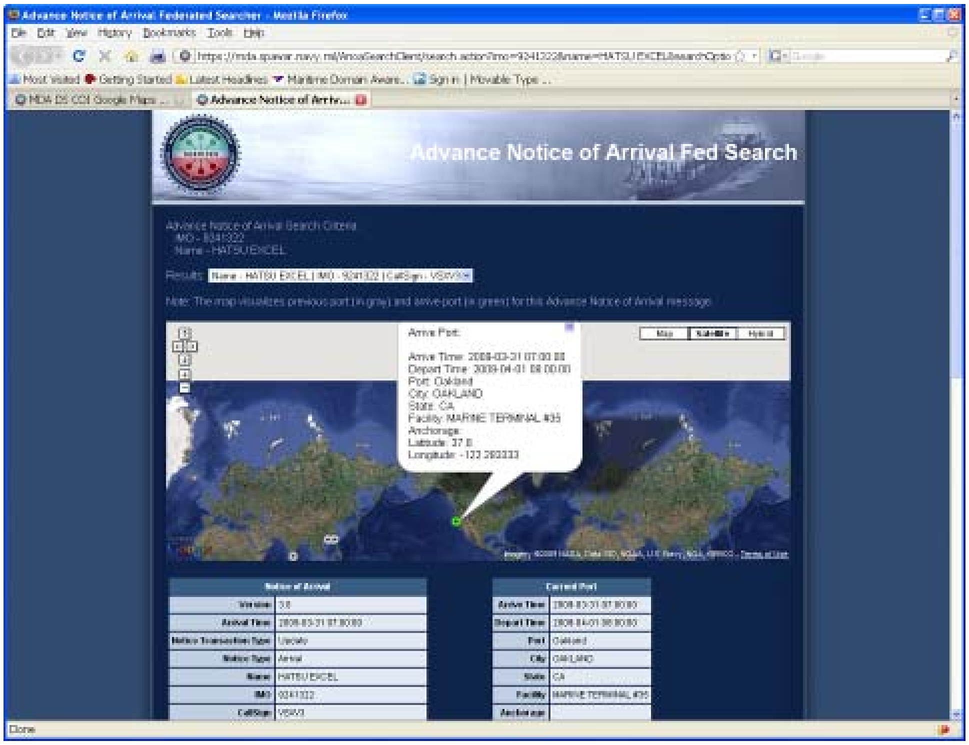
Figure 14. Ship with ANOA tag (HATSU EXCEL).

Figure 15 shows the port of arrival information. The green circle on the map illustrates the arrival port, and the grey circles indicate previous ports during that vessel's voyage.

Figure 16 depicts the Baja Peninsula Channel in GMMS, and the list of vessels on the left illustrates a ship with a VOI tag on it (CARNIVAL PARADISE), indicating SILO data is available for this vessel. For the purposes of the demonstration, VOI/SILO data was fabricated just to demonstrate the process. At this time, SILO data is not available for viewing on GMMS or through a Federated Search query.

The demonstration concluded with an illustration of how ABAC could be employed to determine an individual's access to sensitive data, such as ANOA data. It distinguished between a U.S. citizen in law enforcement, a U.S. citizen associated with MDA but not in law enforcement, and a foreign national. Using ANOA data as an example, the law enforcement was able to access the full ANOA data set, including the PII, whereas the non-law enforcement user could not see the PII. The foreign national user was unable to see any of the ANOA data (See Figure 17.)

Feedback from attendees was quite positive. Spiral 3 was the last of the sponsored prototype efforts for data sharing within the MDA DS COI. Future development of data sharing capabilities should be coordinated within the National MDA Architecture Management Hub.


Advance Notice of Arrival Federated Searcher - Mozilla Firefox
File Edit View History Bookmarks Tools Help
https://mda.spawar.navy.mil/AnoaSearchClient/search.action?imo=9241322&name=HATSU EXCEL&searchOptio
Most Visited Getting Started Latest Headlines Maritime Domain Aware... Sign in | Movable Type ...
MDA DS COI Google Maps ...
Advance Notice of Arriv...
Advance Notice of Arrival Fed Search
Map
Satellite
Hybrid
Done

Advance Notice of Arrival Search Criteria
IMO - 9241322
Name - HATSU EXCEL

Results: Name - HATSU EXCEL | IMO - 9241322 | CallSign - VSXV3

Note: The map visualizes previous port (in gray) and arrive port (in green) for this Advance Notice of Arrival message

Arrive Port:

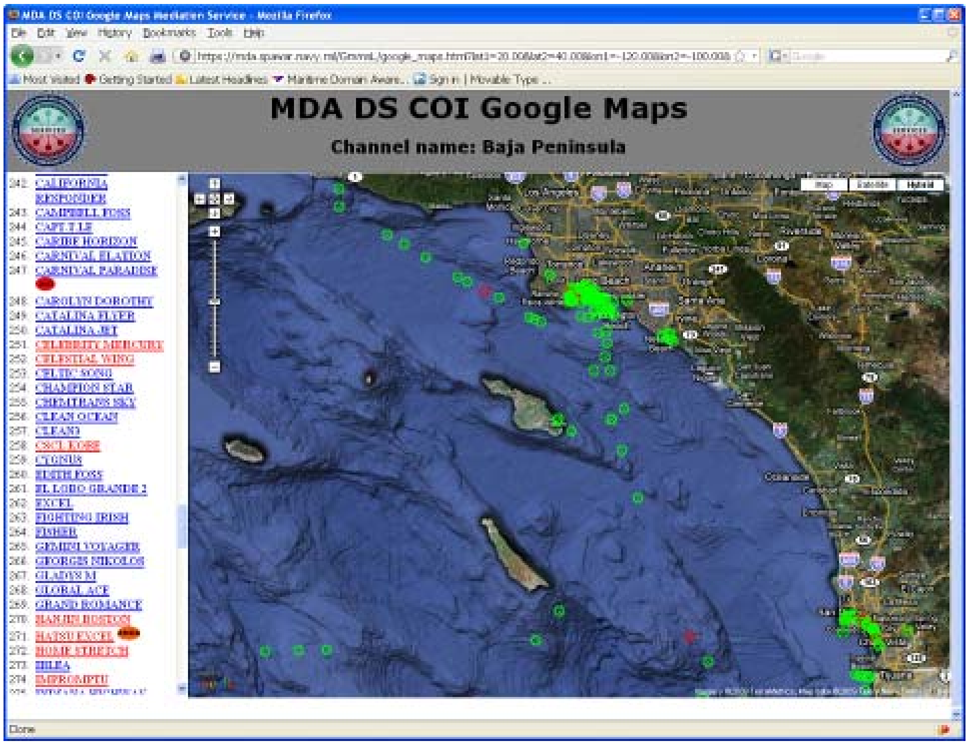
Arrive Time: 2008-03-31 07:00:00
Depart Time: 2008-04-01 08:00:00
Port: Oakland
City: OAKLAND
State: CA
Facility: MARINE TERMINAL #35
Anchorage:
Latitude: 37.8
Longitude: -122.283333

Imagery ©2009 NASA, Data SIO, NOAA, U.S. Navy, NGA, GEBCO - Terms of Use

Notice of Arrival	
Version	3.0
Arrival Time	2008-03-31 07:00:00
Notice Transaction Type	Update
Notice Type	Arrival
Name	HATSU EXCEL
IMO	9241322
CallSign	VSXV3

Current Port	
Arrive Time	2008-03-31 07:00:00
Depart Time	2008-04-01 08:00:00
Port	Oakland
City	OAKLAND
State	CA
Facility	MARINE TERMINAL #35
Anchorage	

Figure 15. ANOA with arrival port (green) and previous ports (grey).


MDA DS COI Google Maps Mediation Service - Mozilla Firefox
File Edit View History Bookmarks Tools Help
Most Visited Getting Started Latest Headlines Maritime Domain Aware... Sign in | Movable Type ...
Map Satellite Hybrid
Los Angeles
Santa Ana
Oceanside
Tijuana
Done

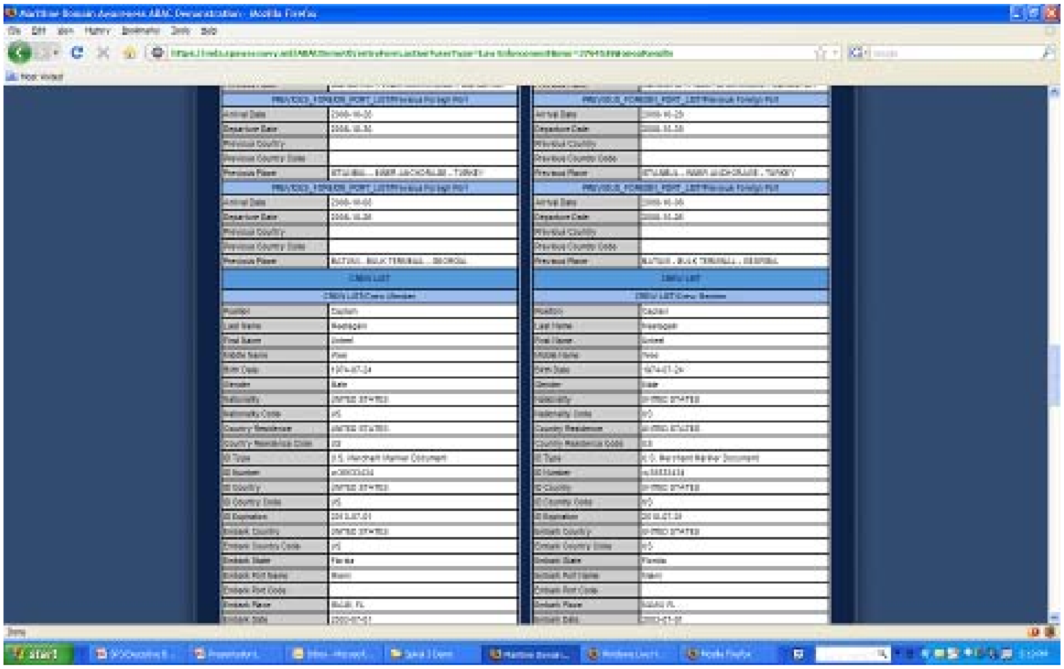
https://mda.spawar.navy.mil/Gmmd.../google_maps.html?lat1=20.00&lat2=40.00&lon1=-120.00&lon2=-100.00

MDA DS COI Google Maps

Channel name: Baja Peninsula

242. CALIFORNIA RESPONDER
243. CAMPBELL FOSS
244. CAPT T LE
245. CARIBE HORIZON
246. CARNIVAL ELATION
247. CARNIVAL PARADISE
248. CAROLYN DOROTHY
249. CATALINA FLYER
250. CATALINA JET
251. CELEBRITY MERCURY
252. CELESTIAL WING
253. CELTIC SONG
254. CHAMPION STAR
255. CHEMTRANS SKY
256. CLEAN OCEAN
257. CLEANO
258. CSCL KOBE
259. CYGNUS
260. EDITH FOSS
261. EL LOBO GRANDE 2
262. EXCEL
263. FIGHTING IRISH
264. FISHER
265. GEMINI VOYAGER
266. GEORGIS NIKOLOS
267. GLADYS M
268. GLOBAL ACE
269. GRAND ROMANCE
270. HANJIN BOSTON
271. HATSU EXCEL
272. HOME STRETCH
273. HILEA
274. IMPROMPTU

Figure 16. Ship with vessel of interest (VOI) tag (CARNIVAL PARADISE).


Maritime Domain Awareness ABAC Demonstration - Mozilla Firefox
File Edit View History Bookmarks Tools Help
Most Visited
Done
start

PREVIOUS_FOREIGN_PORT_LIST/Previous Foreign Port		PREVIOUS_FOREIGN_PORT_LIST/Previous Foreign Port	
Arrival Date	2008-10-20	Arrival Date	2008-10-20
Departure Date	2008.10.30	Departure Date	2008.10.30
Previous Country		Previous Country	
Previous Country Code		Previous Country Code	
Previous Place	ISTANBUL ... [illegible] ANCHORAGE ... TURKEY	Previous Place	ISTANBUL ... [illegible] ANCHORAGE ... TURKEY
PREVIOUS_FOREIGN_PORT_LIST/Previous Foreign Port		PREVIOUS_FOREIGN_PORT_LIST/Previous Foreign Port	
Arrival Date	2008-10-05	Arrival Date	2008-10-05
Departure Date	2008.10.28	Departure Date	2008.10.28
Previous Country		Previous Country	
Previous Country Code		Previous Country Code	
Previous Place	BATUMI ... BULK TERMINAL ... GEORGIA	Previous Place	BATUMI ... BULK TERMINAL ... GEORGIA
CREW LIST		CREW LIST	
CREW LIST/Crew Member		CREW LIST/Crew Member	
Position	Captain	Position	Captain
Last Name	[illegible]	Last Name	[illegible]
First Name	[illegible]	First Name	[illegible]
Middle Name	[illegible]	Middle Name	[illegible]
Birth Date	1974-07-24	Birth Date	1974-07-24
Gender	Male	Gender	Male
Nationality	UNITED STATES	Nationality	UNITED STATES
Nationality Code	US	Nationality Code	US
Country Residence	UNITED STATES	Country Residence	UNITED STATES
Country Residence Code	US	Country Residence Code	US
ID Type	U.S. Merchant Marine Document	ID Type	U.S. Merchant Marine Document
ID Number	[illegible]	ID Number	[illegible]
ID Country	UNITED STATES	ID Country	UNITED STATES
ID Country Code	US	ID Country Code	US
ID Expiration	2013.07.01	ID Expiration	2013.07.01
Embark Country	UNITED STATES	Embark Country	UNITED STATES
Embark Country Code	US	Embark Country Code	US
Embark State	Florida	Embark State	Florida
Embark Port Name	Miami	Embark Port Name	Miami
Embark Port Code		Embark Port Code	
Embark Place	MIAMI, FL	Embark Place	MIAMI, FL
Embark Date	2002-07-01	Embark Date	2002-07-01

Figure 17. ABAC return of the crew information (PII) to a Law Enforcement user.

4 LESSONS LEARNED

The collaborative environment of a COI, with various organizations and agendas, inherently generates a list of things that it did not know or anticipate when it came together. The MDA DS COI is no different. From its beginning with Spiral 1 through the Spiral 3 demonstration, the COI has discovered an abundance of lessons as part of its efforts. This report will concentrate on those lessons associated with Spiral 3.

4.1 Technical

The National Strategy for Data Sharing dictates the use of net-centricity and a SOA environment to facilitate data sharing, which is the basis of the COI's spiral projects. However, NCES and other SOA infrastructures such as Consolidated Afloat Networks and Enterprise Services (CANES) are still evolving. Architecture such as NCES needs to be scalable and flexible to fit the needs of what has been an undefined enterprise. Security models have to be tiered to anticipate and support non-classified data as well as classified and protected data found on classified networks. In a net-centric environment, data providers have to trust the security infrastructure to provide protection for their data, and consumers should have the access they expect and are authorized to receive. The enterprise has to be well defined and an identity management infrastructure has to be in place to support dynamic information sharing policies. All of these developments are occurring in parallel, creating the situation where the developers were working with moving targets in terms of the intended interfaces, services and infrastructures. Interfaces between systems are rapidly changing and must be negotiated. Partnerships and collaboration between the infrastructure developers and the application developers are critical for success. A strong partnership between NCES and the MDS DS COI was the basis of the overall success of the COI.

4.2 Governance

MDA data sharing requires senior leadership support and prioritization. Information sharing is driven by national policy and supports the priorities of the Department. The national imperative for data sharing is reflected in high level IT strategy documents. These needs are often filtering down to established programs as unfunded requirements requiring high-level visibility to justify execution. Senior leadership through the MDA implementation team brought the MDA DS COI together and provided leadership through the approval of Spiral 3. As Spiral 3 progressed, the MDA governance changed from the US Navy - US Coast guard implementation team to a multi agency MDA stakeholder's board. This stakeholder's board while interested, did not have the charter ownership and was not engaged in the progression of the DS COI technical work. This change was reflected in the ability of the MDA DS COI to push the policy issues related to ABAC and put the effort in a mode of following existing policy with little chance for piloting breakthrough in policy/technical approaches.

4.3 Cultural

The culture of data management is based on system-oriented philosophies with stovepipe paradigms not easily broken. Data stewards are responsible for ensuring the security of their data within the confines of policy and regulation. A national policy that dictates net-centric data sharing in an SOA environment is contrary to virtually all legacy systems. Nonetheless, DoD policy mandates net-centric information sharing. Some organizations have willingly complied, but the mandate provides no enforcement mechanism. Other than the documents dictating the policy, there is no method of accountability. Therefore, compliance is evaluated at the institutional level based on the organization's interpretation of net-centricity. Net-centricity requires a framework for access and services that allows system-to-system interaction to meet the needs of a well-defined base of consumers. Resourcing net-centric data sharing is not within normal Program of

Record (POR) boundaries. PORs are not funded for sharing information beyond their program, nor are they normally assigned personnel specifically to support information sharing. That support comes from an organizational commitment to data sharing and an understanding of the importance of MDA. The perception among many in DoD, DHS, and especially organizations outside DoD and DHS, is that "maritime" means Navy and Coast Guard. MDA involves much more than just Navy and Coast Guard. The COI's efforts thus far have proven that maritime interests are across a gamut of organizations at the Federal, state, local, tribal, industry, and international levels.

4.4 Implementation

Implementing new policies and procedures is always risky and challenging. To commit to a new information sharing concept, organizations need support. They may need training or orientation to understand the architecture and infrastructure. They also need assurances that their participation does not jeopardize their organizational security nor compromise their data. Coordination and collaboration is required among data producers, consumers, and providers of Core Enterprise Services (CES). Data producers need to know what consumers need and expect when accessing their data. Providers of CES need to understand the kind of infrastructure that best meets the needs of their constituents. In addition, consumers need to understand the nature of available data sources and the infrastructure in which data is accessible.

A core team of project stakeholders is necessary to bind efforts together in a purposeful, focused way. Such a team has the continuity and expertise to determine the need for collaboration, involvement of leadership, and changes in technical direction. A core team can facilitate communication when needed and serves as the broker for technical, governance, cultural, and implementation issues. For Spiral 3, each organization within the core team had to overcome its own challenges. Funding constraints, key personnel changes, institutional requirements, etc. were obstacles that could have provided a reason to offer minimal support to the project. In spite of these obstacles the team achieved success and laid the foundation for continued development of MDA data sharing.

5 RECOMMENDATIONS

The MDA DS COI developed an effective approach to MDA data sharing. Sharing AIS, ANOA and SILO contributes to interagency awareness of the maritime domain. Just as important is the repeatable process invoked by the COI. Breaking data management, pilot technical and policy into three working groups proved to be an excellent way to divide the work and enable organizations to contribute. Uniting these teams purpose through the phased development of three increasingly complex spirals allowed the effort to discover problems, close gaps and move forward on all fronts. These recommendations reflect Coast Guard experience and opinions.

In Spiral 3 the COI conducted an effective concept demonstration of ABAC as applied to sample NOA data. The ABAC technology was brought up to date from earlier DISA developments and shows great promise for the MDA community. Future efforts should incorporate ABAC into initial phases and create new processes to resolve policy from the onset. Adding access controls as an added feature towards the end of a project allows little time to address policy concerns and construct technical solutions. Access controls affect performance and must be engineered into the solutions from the beginning to ensure adequate performance of the final product.

Enterprise architectures indicate that XML messaging will be an integral part of any MDA data sharing solution. The MDA DS COI application of NCES messaging has scaled up in data quantity faster than NCES can scale the system to accommodate the messaging traffic. Early decisions by the MDA DS COI increased the size of individual messages with more and more descriptive vessel data. While useful for MDA, much of this data was repetitive from message to message and only serves to tax the capacity of NCES messaging. As we go forward, frequent AIS XML messaging payloads need to be reduced to essential event notification information and not regarded as a complete information payload. The additional descriptive vessel data can be ideally provided through a query response service similar to the Historical AIS or the ANOA federated search services. Alternatively, this data can be provided at a less frequent update rate on an additional NCES messaging channel. Alternative messaging infrastructures need to be investigated to support sharing with non-DOD agencies.

At this writing in June 2009, AIS data is being shared by USCG, USN, DOT, and Canada through several data publishing nodes. ANOA (without PII) is being shared by USCG to selected subscribers. The DISA NCES infrastructure is being heavily leveraged to provide system to system messaging. The MDA DS COI core team is funded through September 2009 to support and maintain this capability. If the Coast Guard data sharing established by the MDA DS COI is to continue in FY10 and beyond it must be a planned effort.

On April 15, 2009 the National Maritime Domain Awareness Architecture Management Hub was chartered with the objective: “The Hub shall enhance national maritime domain awareness (MDA) by facilitating the alignment and implementation of standards, processes and technology to improve information and intelligence sharing among the Global Maritime Community of Interest (GMCOI).” This organization has been identified as a transition path for the MDA DS COI. This effort is chartered and conducted with the primary purpose of providing an architecture to enable MDA data sharing. The capabilities and activities of the MDA DS COI core team do not fit with the chartered activity of the National MDA Architecture Management Hub. The Hub does not contain any technical capacity to maintain the data sharing capabilities implemented by the MDA DS COI. Existing and new data sharing efforts should be brought to the attention and coordinated through the Hub to ensure that the new architecture meets interagency requirements.

6 SUMMARY

In Spiral 3 the MDA DS COI extended MDA data sharing beyond the present situation (as reflected in AIS) to future (notice of arrival - ANOA) and actionable information (vessel watch lists - SILO). The effort continued to follow the net-centric data strategy to make sensitive data visible, accessible, and understandable via DISA NCES. Collaboration between and within agencies was very strong. As a result of this project, ANOA data (without PII) is shared with our DOD partners through publication to NCES hourly and is available by query via NCES federated search services. Sharing ANOA data directly (no replication) from within operational Coast Guard systems and allowing protected net-centric access to this information represents a significant achievement in Coast Guard information sharing. It epitomizes the national data sharing strategy and is a major accomplishment to build upon for additional MDA data.

APPENDIX A. MDA DS COI

There are many communities of interest associated with maritime domain awareness, each of which is focused on a particular aspect of MDA. The Data Sharing community was created to ensure knowledge and information was exchanged as freely as possible among MDA stakeholders. In today's world of information technology, sharing information from various systems and networks is no small task. The information below describes the MDA DS COI.

A.1 Charter and Scope

The MDA DS COI was chartered in March 2006 to implement the DoD Net-Centric Data Strategy in accordance with DoD Guide 8320.2-G, *Guidance for Implementing Net-Centric Data Sharing*. The scope of the COI was to exercise responsibility for identifying organizations that provide and use MDA data and information, facilitating resolution of inconsistencies, coordinating data deconfliction with the DoD Registry, and providing implementation guidance to program offices as required. Initially, the COI focused on developing, coordinating, and deconflicting a standardized set of vocabularies and schemas for COI pilot projects.

A.2 MDA DS COI Authority

The COI was established in accordance with the following documentation which also served as the authority for this COI to operate:

- *National Plan to Achieve Maritime Domain Awareness and DoD 8320.2-G*, October 2005
- Joint Requirements Oversight Council (JROCM) memorandum 199-04, *Data Strategy Implementation for Warfighter Domain Systems*, 29 Oct 04
- DoD Chief Memorandum, *DoD Net-Centric Data Strategy*, 9 May 03
- *Department of Defense Net-Centric Data Strategy*, 9 May 03
- DoD Instruction (DoDI) 8320.2, *Data Sharing in a Net-Centric Department of Defense*, 2 Dec 04
- Executive Order 13356, Sec 3, August 27, 2004
- Director of Central Intelligence (DCI) Memo, 4 March 2004, (Unclassified/For Official Use Only (U/FOUO)), *Homeland Security Information Sharing Memorandum of Understanding Between the Intelligence Community, Federal Law Enforcement Agencies and DHS Concerning Information Sharing*
- Public Law 108-458-Dec 17, 2004, *Intelligence Reform and Terrorism Prevention Act of 2004*, Sec 1016, Information Sharing
- Executive Order 13311, July 29, 2003, *Homeland Security Information Sharing*
- Homeland Security Act of 2002, Sec 202 and 892
- Executive Order 12958, April 17, 1995

A.3 MDA DS COI Goals

The goals and objective of the COI were to facilitate/accomplish the following:

- Compile and address information sharing requirements for platforms or agencies operating within the MDA environment.
- Define/implement a work process for fostering COI-wide data sharing and management methods and capabilities.
- Synchronize COI products with DoD Decision Support Systems (i.e., Defense Acquisition System; Planning, Programming, Budgeting & Execution; Joint Capabilities Integration Development System; and other Federal budgetary processes as necessary).
- Develop a shared vocabulary in accordance with DoD Net-Centric Data Strategy that is consistent with non-DoD participants' data strategy.
- Develop repeatable processes that promote community-wide data management and access.
- Influence appropriate programs of record to adopt net-centric data sharing and SOA.
- Facilitate implementation of net-centric data sharing and SOA across the member organizations.

It was to be accomplished by providing a forum for interagency coordination of community standards on how information can be exchanged within the COI. It was to develop a data vocabulary or taxonomy and register the data standards in the DoD Metadata Registries, and promote common vocabulary, taxonomies and data standards among DoD and data standards among DoD and non-DoD participants. Non-DoD Departments and Agencies were able to register with their own data registry.

A.4 Organization

Membership in the COI consisted of three categories: 1) Full Members, 2) Contributing Members, and 3) At-large Members. Full members comprised the COI's leadership and management structure, and fell into one of two groups: management or working groups. Contributing Members and At-large Members were non-voting members who were involved with producing or consuming MDA data, would provide subject matter expertise, etc.

A.5 MDA DS COI Management

The Management hierarchy of the MDA DS COI consists of an Executive Board and a Steering Committee. The hierarchy of the COI, including the Working Groups, is shown in Figure A-1.

A.5.1 Executive Board

The Executive Board was made up of a senior member each from DoD and DHS. Their role was to ensure the COI incorporated a data strategy that was compliant with overarching DoD and DHS visions of a shared information environment as it applied specifically to the maritime domain. The senior advisors also provided advocacy, as required, to secure necessary resources that enabled the COI to meet its mission.

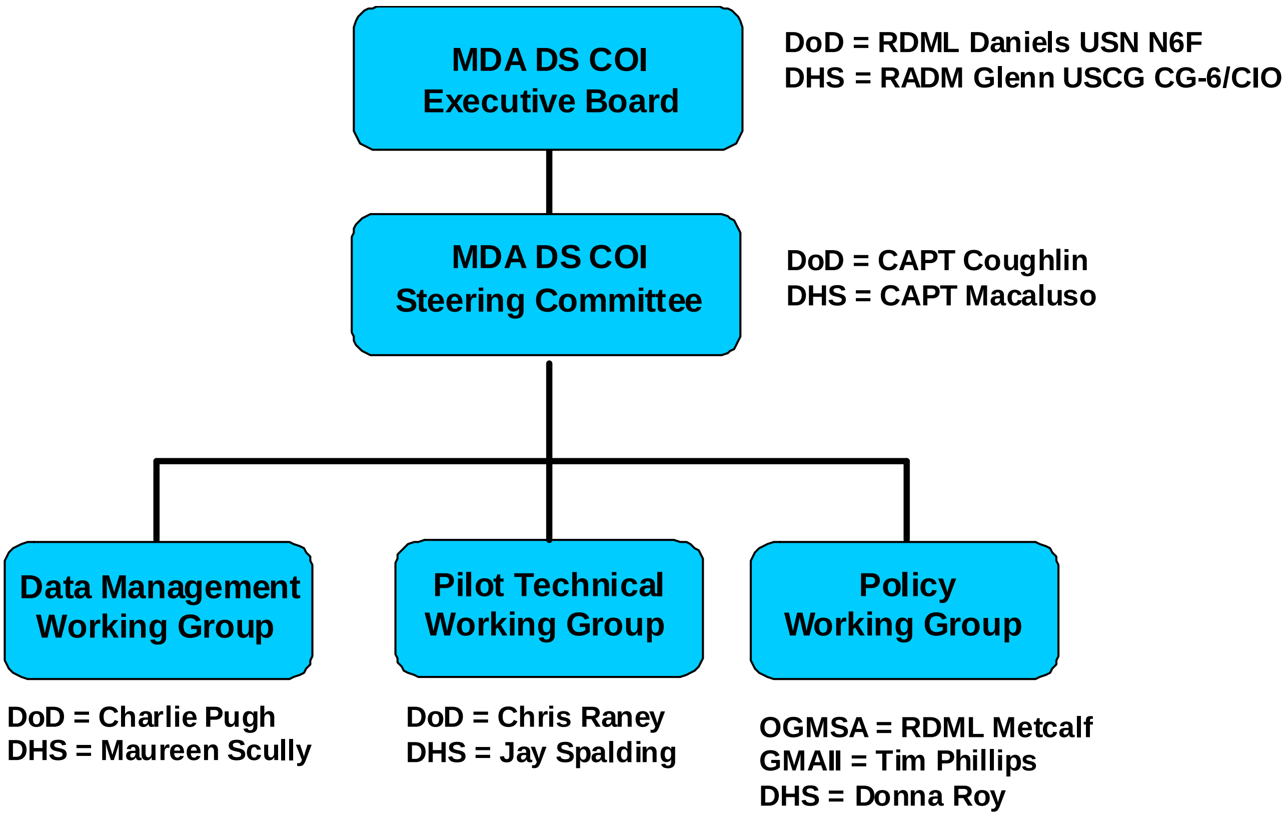


Figure A-1. MDA DS COI governance.

A.5.2 Steering Committee

The Steering Committee was chaired by senior members (O6/GS-15) from DoD and DHS. Its primary task was to keep the COI efforts focused on tasks from the MDA-Implementation Team and other relevant issues. The Steering Committee reviewed and adjudicated COI conflicts and advocate for organizational implementation and support.

A.6 Working Groups

Working Group requirements were directed by the Steering Committee to address specific actions delineated in DoD Guide 8320.2-G, *Guidance for Implementing Net-Centric Data Sharing*. Group leadership was primarily from DoD and DHS, but came from other departments and agencies as appropriate. There were three static working groups, but other sub-groups were assigned as necessary.

A.6.1 Data Management Working Group

The DMWG was established in February 2006 to develop the MDA COI Pilot core vocabulary, data models, and schemas. An emphasis was placed on defining and developing key data objects to include conveyance, cargo, and people. The (defined) scope of the pilot effort integrated data from three separate AIS data providers. The DMWG developed shared vocabulary for the Maritime Domain problem area in accordance with DoD Net-Centric Data Strategy and other Government data management guidance.

The MDA COI Pilot was aligned with the core MDA-Implementation Team. The MDA COI DMWG co-chairs represented both the DoD, USN component, and the DHS, USCG component. Within the DMWG, technical support was provided by the MITRE Corporation.

The primary organizations involved in the DMWG were:

- Commercial partners
- CMA JCTD
- DISA
- DHS Office of the Chief Information Officer (OCIO)/Enterprise Data Management Office (EDMO)
- ONI
- U.S. Navy/Operational Navy (OPNAV)
- National Maritime Intelligence Center (NMIC)
- Naval Postgraduate School (NPS)
- Naval Research Laboratory (NRL)
- Office of Naval Research (ONR)
- Project SeaHawk
- USCG

A.6.2 Policy Working Group

The PWG determined the need to establish data sharing requirements to ensure the data that could be shared was available to consumers, and any restrictions to sharing data were published to the COI. The PWG was responsible for establishing the following:

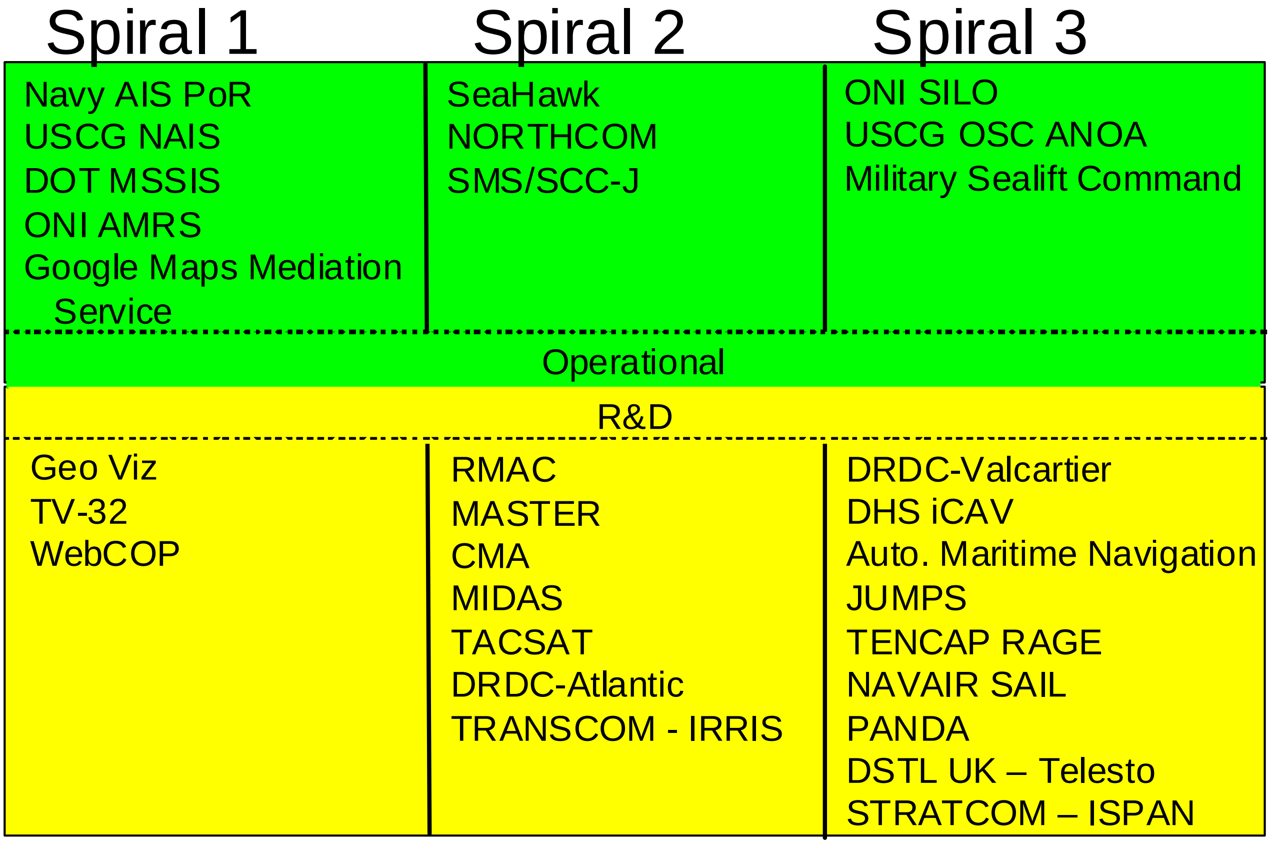
- Business rules/security policies for sharing of personal information
- NCES governance structure
- What information could be shared freely
- What information could be shared only with designated personnel/groups
- What information could not be shared
- What monitoring/testing was required to ensure information sharing policies were met

A.6.3 Pilot Technical Working Group

The PTWG was responsible for developing repeatable processes and capabilities to demonstrate COI products (i.e., data vocabulary, enterprise services, UDOP). The PTWG was comprised of Navy and Coast Guard SMEs, with contractor support from Solers, Inc. (Navy) and Science Applications International Corporation (SAIC) (Coast Guard). The PTWG was tasked with developing solutions to complex technical problems and was an integral part of the success of the Spiral projects.

A.7 Net-Centric Coalition of the Willing

At the beginning of the MDA DS COI, a few organizations were willing to support the projects as either producers or consumers. As the efforts progressed, the number of participants increased significantly, representing a cross-section of organizations that either produced valuable information or had a need for the information; and, in some cases, both. These organizations willingly participated with the COI because of the value of information sharing and its implication for better situational awareness in the future. They became part of a "net-centric coalition of the willing" intent on sharing MDA data. Figure A-2 shows the members of this coalition.



Spiral 1	Spiral 2	Spiral 3
Navy AIS PoR USCG NAIS DOT MSSIS ONI AMRS Google Maps Mediation Service	SeaHawk NORTHCOM SMS/SCC-J	ONI SILO USCG OSC ANOA Military Sealift Command
Operational		
R&D		
Geo Viz TV-32 WebCOP	RMAC MASTER CMA MIDAS TACSAT DRDC-Atlantic TRANSCOM - IRRIS	DRDC-Valcartier DHS iCAV Auto. Maritime Navigation JUMPS TENCAP RAGE NAVAIR SAIL PANDA DSTL UK – Telesto STRATCOM – ISPAN

Figure A-2. Net-centric coalition of the willing.

A.8 MDA DS COI History

The COI began during an MDA conference in February 2006, followed closely in March 2006 by the kickoff of the Spiral 1 effort: proving MDA data could be shared net-centrically in a services-oriented environment. In October and again in December 2006, the COI successfully demonstrated that AIS data could be exposed on an enterprise network (NCES) and freely accessed by anyone with proper authorization (CAC/PKI certification). Spiral 2 began in April 2007 with the goal of enhancing AIS data with value-added services that included data augmentation, historical archiving, and anomaly detection. During this effort, the National Concept of Operations (CONOPS) was established and the DoD Executive Agent for MDA was designated (August 2007). Knowing that data sharing capabilities would continue to grow, Spiral 3 started in January 2008 with the goal of adding data sources that were sensitive in nature and thus needing access controls beyond a CAC or PKI certification. NOA data and SILO data were selected as the new data sources because of the sensitivity of the information. ABAC was selected as the control standard to ensure only those with proper credentials could access NOA or SILO data. In April 2008, the DHS Executive Agent for MDA was designated. Spiral 2 was successfully demonstration in April 2008 as well. Development efforts continued through 2008, despite delays due to policy concerns and technical difficulties with the NCES messaging services. In December 2008, the Navy MDA Office was established, which set the stage for continued development in the future. Finally, in March 2009, Spiral 3 was demonstrated to a senior DoD/DHS audience, illustrating a mechanism through which sensitive data could be shared and protected at the same time. Not all Spiral 3 goals were met, but the concepts behind the goals were proven valid. Figure A-3 shows the history of the MDA DS COI.

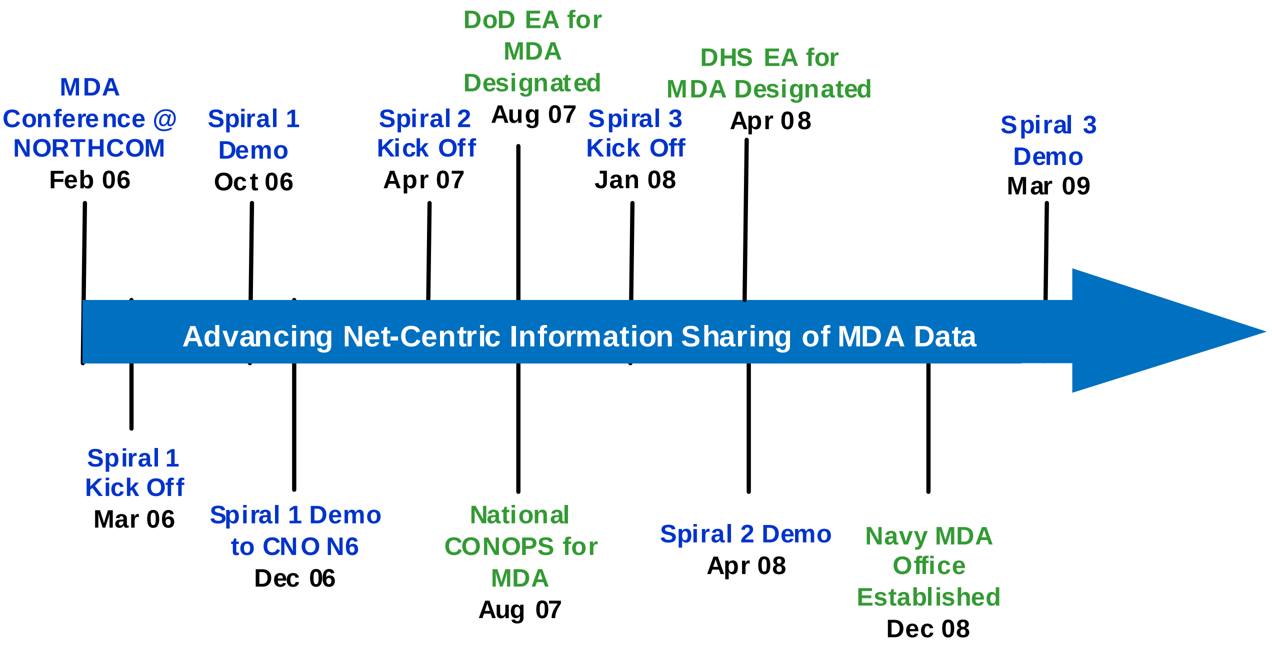


Figure A-3. History of the MDA DS COI.

APPENDIX B. DATA SHARING POLICY FRAMEWORK

Table B-1. Information sharing framework for USCG-ANOA.

Contact Information

USCG-ANOA Technical POC Name	Joe Sargent
USCG-ANOA Technical POC Phone	202-372-2795
USCG-ANOA Technical POC Email	Joseph.P.Sargent@uscg.mil
USCG-ANOA Policy POC Name	Same as above; Alternate Beth Crowley
USCG-ANOA Policy POC Phone	202-475-3493
USCG-ANOA Policy POC Email	Beth.Crowley@uscg.mil

Identify What Information Can Be Shared With Whom

	Information Sharing Authorized															
Data To Be Shared	No Sharing Restrictions	DOD	USCG	DHS	DOJ	DOS	DOT	Other US Gov't	Law Enforcement	Intelligence	Canada	UK	Australia	New Zealand	Other 1	Other 2
Vessel Name		X	X	X	X	X	X	X	X	X						
Call Sign		X	X	X	X	X	X	X	X	X						
Vessel ID Number		X	X	X	X	X	X	X	X	X						
Country of Registry		X	X	X	X	X	X	X	X	X						
Registered Owner		X	X	X	X	X	X	X	X	X						
Operator		X	X	X	X	X	X	X	X	X						
Classification Society		X	X	X	X	X	X	X	X	X						
DOCUMENT OF COMPLIANCE CERTIFICATE		X	X	X	X	X	X	X	X	X						
Date of Issuance		X	X	X	X	X	X	X	X	X						
Issuing Agency		X	X	X	X	X	X	X	X	X						
SAFETY MANAGEMENT CERTIFICATE		X	X	X	X	X	X	X	X	X						
Date of Issuance		X	X	X	X	X	X	X	X	X						
Issuing Agency		X	X	X	X	X	X	X	X	X						
Operational Condition of Equipment		X	X	X	X	X	X	X	X	X						
Reporting Party Name		X	X	X	X	X	X	X	X	X						
Reporting Party Company		X	X	X	X	X	X	X	X	X						
Reporting Party Telephone Number		X	X	X	X	X	X	X	X	X						
Name of Vessel's Charterer		X	X	X	X	X	X	X	X	X						
Vessel's Current Position		X	X	X	X	X	X	X	X	X						
Date & Time of Report		X	X	X	X	X	X	X	X	X						
U.S. Destination Port or Place/City & State		X	X	X	X	X	X	X	X	X						
Estimated Date & Time of Arrival		X	X	X	X	X	X	X	X	X						
Estimated Date & Time of Departure		X	X	X	X	X	X	X	X	X						
U.S. Destination Receiving Facility/Terminal/Anchorage		X	X	X	X	X	X	X	X	X						
U.S. Coast Guard Captain of the Port (COTP) Zone		X	X	X	X	X	X	X	X	X						
Point of Contact (POC)		X	X	X	X	X	X	X	X	X						
POC 24 Hour Telephone Number		X	X	X	X	X	X	X	X	X						
POC Fax Number		X	X	X	X	X	X	X	X	X						

Table B-1. Information sharing framework for USCG-ANOA (Continued).

Identify What Information Can Be Shared With Whom																
CONSECUTIVE PORTS OF CALL FOR CURRENT VOYAGE		X	X	X	X	X	X	X	X	X						
Receiving Facility		X	X	X	X	X	X	X	X	X						
Port or Place		X	X	X	X	X	X	X	X	X						
City &State		X	X	X	X	X	X	X	X	X						
24-Hour POC (Name & Telephone Number)		X	X	X	X	X	X	X	X	X						
Est Date & Time of Arrival		X	X	X	X	X	X	X	X	X						
Est Date & Time of Departure		X	X	X	X	X	X	X	X	X						
CARGO AND PREVIOUS PORTS		X	X	X	X	X	X	X	X	X						
General Description of Cargo		X	X	X	X	X	X	X	X	X						
Cargo Amount		X	X	X	X	X	X	X	X	X						
Certain Dangerous Cargo (CDC) Onboard?		X	X	X	X	X	X	X	X	X						
Last Five Ports/Places Visited		X	X	X	X	X	X	X	X	X						
Date of Arrival		X	X	X	X	X	X	X	X	X						
Date of Departure		X	X	X	X	X	X	X	X	X						
INTERNATIONAL SHIP SECURITY CERTIFICATE		X	X	X	X	X	X	X	X	X						
Date of Issuance		X	X	X	X	X	X	X	X	X						
ISSC Type (CG Approved VSP, Interim ISSC, Final ISSC)		X	X	X	X	X	X	X	X	X						
Vessel Security Plan Implemented?		X	X	X	X	X	X	X	X	X						
If an Interim ISSC was issued, choose/indicate reason		X	X	X	X	X	X	X	X	X						
Flag Administration or RSO		X	X	X	X	X	X	X	X	X						
COMPANY SECURITY OFFICER (CSO)									**X**							
CSO Name									**X**							
24 Hour Telephone Number									**X**							
Email Address									**X**							
CREW LIST									**X**							
Name in Full (Family Name, Given Name and Initial)									**X**							
Date of Birth									**X**							
Nationality									**X**							
Identification (ID) Passport or Merchant Mariner's Doc									**X**							
Position or Duties									**X**							
Where Embarked (Port or Place & Country)		X	X	X	X	X	X	X	**X**	X						
NON-CREW AND PASSENGER LIST									**X**							
Name in Full (Family Name, Given Name and Initial)									**X**							
Date of Birth									**X**							
Nationality									**X**							
Identification (ID) Passport or Merchant Mariner's Doc									**X**							
Where Embarked (Port or Place & Country)		X	X	X	X	X	X	X	**X**	X						
CERTAIN DANGEROUS CARGO LIST		X	X	X	X	X	X	X	X	X						
Name of Certain Dangerous Cargo		X	X	X	X	X	X	X	X	X						
Amount		X	X	X	X	X	X	X	X	X						
Offload Port		X	X	X	X	X	X	X	X	X						
UN Number		X	X	X	X	X	X	X	X	X						
VESSEL ARRIVAL/DEPARTURE UPDATE		X	X	X	X	X	X	X	X	X						
Vessel Name		X	X	X	X	X	X	X	X	X						

Table B-1. Information sharing framework for USCG-ANOA (Continued).

Call Sign		X	X	X	X	X	X	X	X	X						
Vessel ID Number		X	X	X	X	X	X	X	X	X						
Country of Registry		X	X	X	X	X	X	X	X	X						
Date of Original Report		X	X	X	X	X	X	X	`	X						
Time of Original Report		X	X	X	X	X	X	X	X	X						
Vessel's Original Destination		X	X	X	X	X	X	X	X	X						
Type of Changes Included in this Report (Destination, ETA, Voyage Info, ETD, Crew, Cargo, 24-Hour POC, Other(specify)		X	X	X	X	X	X	X	X	X						
Changes Additions or Deletions		X	X	X	X	X	X	X	X	X						
Action (Change, Additions or Deletions)		X	X	X	X	X	X	X	X	X						
Type of Change		X	X	X	X	X	X	X	X	X						
Change from:		X	X	X	X	X	X	X	X	X						
Change To:		X	X	X	X	X	X	X	X	X						

Identify information sharing restrictions, recommend attributes to enforce information sharing restrictions, and determine risk if data is share

Data To Be Shared	Information Sharing Restrictions	Attributes Needed to enforce ABAC	Risk If Data Is Shared
Vessel Name			
Call Sign			
Vessel ID Number			
Country of Registry			
Registered Owner			
Operator			
Classification Society			
DOCUMENT OF COMPLIANCE CERTIFICATE			
Date of Issuance			
Issuing Agency			
SAFETY MANAGEMENT CERTIFICATE			
Date of Issuance			
Issuing Agency			
Operational Condition of Equipment			
Reporting Party Name			
Reporting Party Company			
Reporting Party Telephone Number			
Name of Vessel's Charterer			
Vessel's Current Position			
Date & Time of Report			
U.S. Destination Port or Place/City & State			
Estimated Date & Time of Arrival			
Estimated Date & Time of Departure			
U.S. Destination Receiving Facility/Terminal/Anchorage			
U.S. Coast Guard Captain of the Port (COTP) Zone			
Point of Contact (POC)			
POC 24 Hour Telephone Number			
POC Fax Number			
CONSECUTIVE PORTS OF CALL FOR CURRENT VOYAGE			
Receiving Facility			

Table B-1. Information sharing framework for USCG-ANOA (Continued).

Port or Place			
City &State			
24-Hour POC (Name & Telephone Number)			
Est Date & Time of Arrival			
Est Date & Time of Departure			
CARGO AND PREVIOUS PORTS			
General Description of Cargo			
Cargo Amount			
Certain Dangerous Cargo (CDC) Onboard?			
Last Five Ports/Places Visited			
Date of Arrival			
Date of Departure			
INTERNATIONAL SHIP SECURITY CERTIFICATE			
Date of Issuance			
ISSC Type (CG Approved VSP, Interim ISSC, Final ISSC)			
Vessel Security Plan Implemented?			
If an Interim ISSC was issued, choose/indicate reason			
Flag Administration or RSO			
COMPANY SECURITY OFFICER (CSO)	Personally Identifiable Information (PII); Governed by MAGNet system policy and related documents: 1). Privacy Impact Assessment (PIA) and 2). System of Records Notice (SORN)	US Citizenship; Law Enforcement (Federal, State, & local); Organization; clearance, etc.	
CSO Name	(same as above - PII)	See above	
24 Hour Telephone Number	(same as above - PII)	See above	
Email Address	(same as above - PII)	See above	
CREW LIST	(same as above - PII)	See above	
Name in Full (Family Name, Given Name and Initial)	(same as above - PII)	See above	
Date of Birth	(same as above - PII)	See above	
Nationality	(same as above - PII)	See above	
Identification (ID) Passport or Merchant Mariner's Doc	(same as above - PII)	See above	
Position or Duties	(same as above - PII)	See above	
Where Embarked (Port or Place & Country)	N/A	N/A	
NON-CREW AND PASSENGER LIST	(same as above - PII)	See above	
Name in Full (Family Name, Given Name and Initial)	(same as above - PII)	See above	
Date of Birth	(same as above - PII)	See above	
Nationality	(same as above - PII)	See above	
Identification (ID) Passport or Merchant Mariner's Doc	(same as above - PII)	See above	
Where Embarked (Port or Place & Country)	N/A	N/A	
CERTAIN DANGEROUS CARGO LIST			
Name of Certain Dangerous Cargo			
Amount			
Offload Port			
UN Number			
VESSEL ARRIVAL/DEPARTURE UPDATE			
Vessel Name			
Call Sign			

Table B-1. Information sharing framework for USCG-ANOA (Continued).

Vessel ID Number			
Country of Registry			
Date of Original Report			
Time of Original Report			
Vessel's Original Destination			
Type of Changes Included in this Report (Destination, ETA, Voyage Info, ETD, Crew, Cargo, 24-Hour POC, Other(specify)			
Changes Additions or Deletions			
Action (Change, Additions or Deletions)			
Type of Change			
Change from:			
Change To:			
Any other unique information sharing restrictions			

Table B-2. Information sharing framework for ONI-SILO (at the UNCLAS NIPRNET security domain).

Contact Information	
ONI-SILO Technical POC Name	Joseph Pecore
ONI-SILO Technical POC Phone	301 669 4207
ONI-SILO Technical POC Email	joseph.pecore@L-3Com.com
ONI-SILO Policy POC Name	Charles Pugh
ONI-SILO Policy POC Phone	301 669-4595
ONI-SILO Policy POC Email	cpugh@nmic.navy.mil

Identify What Information Can Be Shared With Whom

Data To Be Shared	Information Sharing Authorized															
	No Sharing Restrictions	DOD	USCG	DHS	DOJ	DOS	DOT	Other US Gov't	Law Enforcement	Intelligence	Canada	UK	Australia	New Zealand	Other 1	Other 2
WatchListName	See Below	None	None	None	None	None	None	None	None	None	None	None	None	None	Restrict	Restrict
POC	See Below	None	None	None	None	None	None	None	None	None	None	None	None	None	Restrict	Restrict
POCemail	See Below	None	None	None	None	None	None	None	None	None	None	None	None	None	Restrict	Restrict
Organization	See Below	None	None	None	None	None	None	None	None	None	None	None	None	None	Restrict	Restrict
OrgLink	See Below	None	None	None	None	None	None	None	None	None	None	None	None	None	Restrict	Restrict
Shipname	See Below	None	None	None	None	None	None	None	None	None	None	None	None	None	Restrict	Restrict
Concern	See Below	None	None	None	None	None	None	None	None	None	None	None	None	None	Restrict	Restrict
Threat	See Below	None	None	None	None	None	None	None	None	None	None	None	None	None	Restrict	Restrict
Priority	See Below	None	None	None	None	None	None	None	None	None	None	None	None	None	Restrict	Restrict
SCONUM	See Below	None	None	None	None	None	None	None	None	None	None	None	None	None	Restrict	Restrict
MMSI	See Below	None	None	None	None	None	None	None	None	None	None	None	None	None	Restrict	Restrict
Links	See Below	None	None	None	None	None	None	None	None	None	None	None	None	None	Restrict	Restrict
Action	See Below	None	None	None	None	None	None	None	None	None	None	None	None	None	Restrict	Restrict
Flag	See Below	None	None	None	None	None	None	None	None	None	None	None	None	None	Restrict	Restrict
Ship Type	See Below	None	None	None	None	None	None	None	None	None	None	None	None	None	Restrict	Restrict
IMO (ship identification number)	See Below	None	None	None	None	None	None	None	None	None	None	None	None	None	Restrict	Restrict
NeedBy	See Below	None	None	None	None	None	None	None	None	None	None	None	None	None	Restrict	Restrict
Position (lat/lon)	See Below	None	None	None	None	None	None	None	None	None	None	None	None	None	Restrict	Restrict
Position (Date Time)	See Below	None	None	None	None	None	None	None	None	None	None	None	None	None	Restrict	Restrict
Images Link	See Below	None	None	None	None	None	None	None	None	None	None	None	None	None	Restrict	Restrict
CallSign	See Below	None	None	None	None	None	None	None	None	None	None	None	None	None	Restrict	Restrict
NeedBy (The date that the "action" is needed by)	See Below	None	None	None	None	None	None	None	None	None	None	None	None	None	Restrict	Restrict

Table B-2. Information sharing framework for ONI-SILO (at the UNCLAS NIPRNET security domain) (Continued).

Identify information sharing restrictions, recommend attributes to enforce information sharing restrictions, and determine risk if data is share			
Data To Be Shared	**Information Sharing Restrictions**	**Attributes Needed to enforce ABAC**	**Risk If Data Is Shared**
WatchListName	Security and "other" countries	CAPCO	Security violations
POC	Security and "other" countries	CAPCO	Security violations
POCemail	Security and "other" countries	CAPCO	Security violations
Organization	Security and "other" countries	CAPCO	Security violations
OrgLink	Security and "other" countries	CAPCO	Security violations
Shipname	Security and "other" countries	CAPCO	Security violations
Concern	Security and "other" countries	CAPCO	Security violations
Threat	Security and "other" countries	CAPCO	Security violations
Priority	Security and "other" countries	CAPCO	Security violations
SCONUM	Security and "other" countries	CAPCO	Security violations
MMSI fou	Security and "other" countries	CAPCO	Security violations
Action	Security and "other" countries	CAPCO	Security violations
Links	Security and "other" countries	CAPCO	Security violations
Action	Security and "other" countries	CAPCO	Security violations
Flag	Security and FOUO restrictions	CAPCO and FOUO restrictions	Security violations/Administrative procedure violation
Ship Type	Security and FOUO restrictions	CAPCO and FOUO restrictions	Security violations/Administrative procedure violation
IMO (ship identification number)	Security and FOUO restrictions	CAPCO and FOUO restrictions	Security violations/Administrative procedure violation
NeedBy	Security and "other" countries	CAPCO	Security violations
Position (lat/lon)	Security and "other" countries	CAPCO	Security violations
Position (Date Time)	Security and "other" countries	CAPCO	Security violations
Images Link	Security and "other" countries	CAPCO	Security violations
CallSign	Security and FOUO restrictions	CAPCO and FOUO restrictions	Security violations/Administrative procedure violation
NeedBy (The date that the "action" is needed by)	Security and "other" countries	CAPCO	Security violations

Any other unique information sharing restrictions

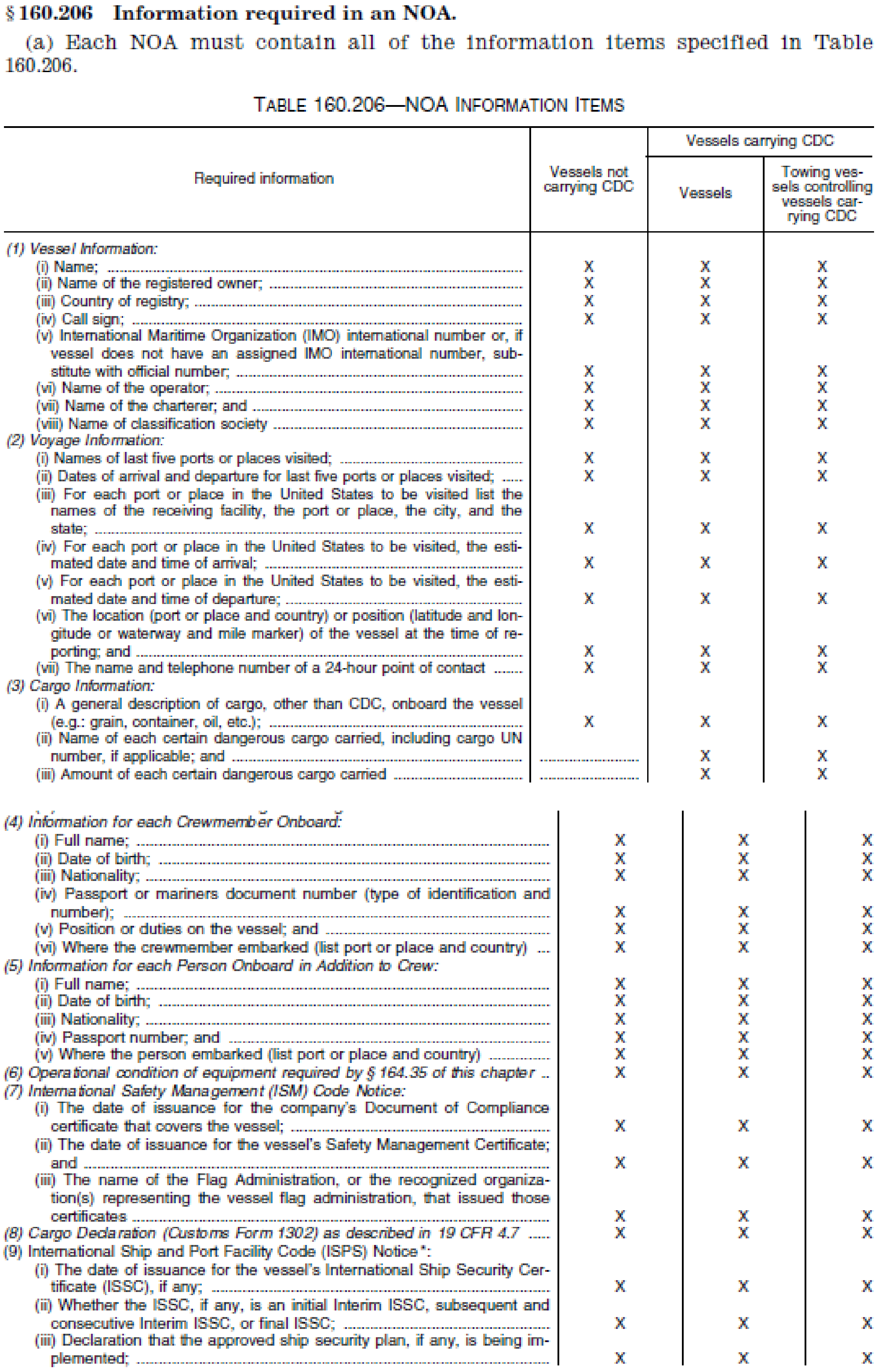
CLASSIFICATION RESTRICTION: If any of the SILO fields for a specific vessel on the list are classified, then all associated fields in the SILO record shall also be treated as classified and shall not be authorized to be viewed in the Unclassified domain. Attributes required to support this level of information sharing are the CAPCO markings. Any ONI SILO entries with CAPCO markings of SECRET or higher shall not be moved to the unclassified level.

DATA SHARING RESTRICTION: An overall caveat of For Official Use Only "FOUO" shall be placed on the SILO fields including "Flag, "Ship Type", "IMO", "CallSign" entries. These fields may not be shared with any non-US government agency.

ADDITIONAL BLANKET DATA SHARING RESTRICTION: Note that all SILO fields from ONI are "Restricted" from "other" data sharing outside those countries specifically listed on the form. Any additional sharing must be coordinated with ONI.

This page intentionally left blank.

APPENDIX C. NOTICE OF ARRIVAL (NOA)



§ 160.206 Information required in an NOA.

(a) Each NOA must contain all of the information items specified in Table 160.206.

TABLE 160.206—NOA INFORMATION ITEMS

Required information	Vessels not carrying CDC	Vessels carrying CDC	
		Vessels	Towing vessels controlling vessels carrying CDC
(1) Vessel Information:			
(i) Name;	X	X	X
(ii) Name of the registered owner;	X	X	X
(iii) Country of registry;	X	X	X
(iv) Call sign;	X	X	X
(v) International Maritime Organization (IMO) international number or, if vessel does not have an assigned IMO international number, substitute with official number;	X	X	X
(vi) Name of the operator;	X	X	X
(vii) Name of the charterer; and	X	X	X
(viii) Name of classification society	X	X	X
(2) Voyage Information:			
(i) Names of last five ports or places visited;	X	X	X
(ii) Dates of arrival and departure for last five ports or places visited;	X	X	X
(iii) For each port or place in the United States to be visited list the names of the receiving facility, the port or place, the city, and the state;	X	X	X
(iv) For each port or place in the United States to be visited, the estimated date and time of arrival;	X	X	X
(v) For each port or place in the United States to be visited, the estimated date and time of departure;	X	X	X
(vi) The location (port or place and country) or position (latitude and longitude or waterway and mile marker) of the vessel at the time of reporting; and	X	X	X
(vii) The name and telephone number of a 24-hour point of contact	X	X	X
(3) Cargo Information:			
(i) A general description of cargo, other than CDC, onboard the vessel (e.g.: grain, container, oil, etc.);	X	X	X
(ii) Name of each certain dangerous cargo carried, including cargo UN number, if applicable; and	....	X	X
(iii) Amount of each certain dangerous cargo carried	....	X	X
(4) Information for each Crewmember Onboard:			
(i) Full name;	X	X	X
(ii) Date of birth;	X	X	X
(iii) Nationality;	X	X	X
(iv) Passport or mariners document number (type of identification and number);	X	X	X
(v) Position or duties on the vessel; and	X	X	X
(vi) Where the crewmember embarked (list port or place and country)	X	X	X
(5) Information for each Person Onboard in Addition to Crew:			
(i) Full name;	X	X	X
(ii) Date of birth;	X	X	X
(iii) Nationality;	X	X	X
(iv) Passport number; and	X	X	X
(v) Where the person embarked (list port or place and country)	X	X	X
(6) Operational condition of equipment required by § 164.35 of this chapter	X	X	X
(7) International Safety Management (ISM) Code Notice:			
(i) The date of issuance for the company's Document of Compliance certificate that covers the vessel;	X	X	X
(ii) The date of issuance for the vessel's Safety Management Certificate; and	X	X	X
(iii) The name of the Flag Administration, or the recognized organization(s) representing the vessel flag administration, that issued those certificates	X	X	X
(8) Cargo Declaration (Customs Form 1302) as described in 19 CFR 4.7	X	X	X
(9) International Ship and Port Facility Code (ISPS) Notice*:			
(i) The date of issuance for the vessel's International Ship Security Certificate (ISSC), if any;	X	X	X
(ii) Whether the ISSC, if any, is an initial Interim ISSC, subsequent and consecutive Interim ISSC, or final ISSC;	X	X	X
(iii) Declaration that the approved ship security plan, if any, is being implemented;	X	X	X

Figure C-1. Extraction from Title 33, CFR, Part 160 describing the required contents of an NOA.

This page intentionally left blank.

APPENDIX D. SPIRAL 3 SCHEMAS

.1 Schemas

.1.1 MIEM

In October 2006, after the completion of MDA DS COI Spiral 1, the DMWG began to collaborate with the CMA Advanced Concept Technology Demonstration (ACTD) on development of the MIEM. The goal was to provide detailed elements for the key constructs of the maritime domain: vessels, cargo, people, and facilities.

The MIEM provides an information exchange model for vessels, cargo, people, and facilities. Therefore, modeling ANOA via the MIEM did not require significant effort. For visualization purposes, the DMWG generated a conceptual model that highlights the primary constructs within a Notice of Arrival (see APPENDIX C). However, as mentioned, the diagram in Figure D-1 is for conceptual visualization and does not focus on ANOA implementation details.

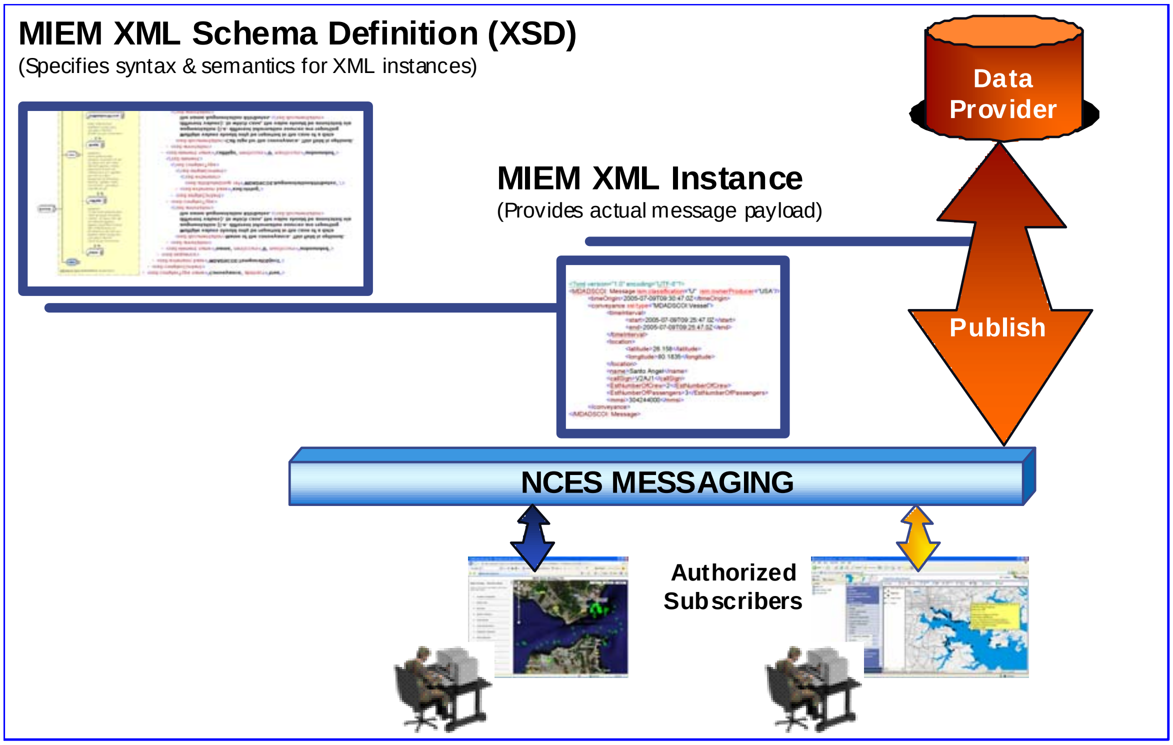

MIEM XML Schema Definition (XSD)
(Specifies syntax & semantics for XML instances)
Data Provider
MIEM XML Instance
(Provides actual message payload)
Publish
NCES MESSAGING
Authorized Subscribers

Figure D-1. Relationship among XSDs, XML instances, data providers/subscribers, and NCES messaging.

.1.1.1 *MIEM Usage Overview*

When using MIEM to send a message, the message body is contained in a <md:payloadFocus> element, which serves as the overall container for any message in MIEM. It takes the form shown in Figure D-2.

```xml
<?xml version="1.0" encoding="UTF-8"?>
<md:payloadFocus
        xsi:schemaLocation="../0.90/miem.xsd"
        xmlns:md="http://miem.gov/md"
        xmlns:sec="urn:us:gov:ic:ism:v2"
        xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">

        <md:section sectionPurpose="assertion">
                <md:element>
                        <md:noticeOfArrival />
                </md:element>
        </md:section>
</md:payloadFocus>
```

Figure D-2. Basic MIEM message structure.

Each <md:payloadFocus> element can contain any number of <md:section> elements. These sections have one of three purposes:

1. To make assertions
2. To provide a list of things that are referenced within the assertion, hereafter referred to as Reference Objects (e.g., vessels, cargo, people)
3. To specify a request for information

In an <md:payloadFocus> element, only a single <md:section> is required. Any given message is not required to contain more than one section, nor required to contain sections of all three types.

Each <md:section> element can contain a number of individual <md:element> structures that contain the actual primary MIEM objects:

- boardingInspection
- cargoEquipment
- cargoManifest
- cargoObject
- cargoShipment
- conveyance
- declarationSubmission
- document
- facility
- noticeOfArrival
- organization
- person
- port
- vessel

The ANOA message (Figure D-3) is laid out in this format because the MIEM relies heavily on the concept of reference objects, where many elements within the primary message body are actually references to other elements contained within the <md:section sectionPurpose=”reference objects”> elements. MIEM messages are made up of a series of self-contained objects that reference each other to build complete messages. MIEM elements are built around the concept of elements having an md:id attribute that uniquely identifies that element, and allows it to be referenced from elsewhere within the document by other elements using the md:ref attribute. This design results in messages where logical objects are physically separated within the XML document, and the logical objects can be reused easily within the message body.

The <md:section> element which has the purpose “assertion” contains the actual Notice of Arrival message, shown in Figure D-4. Figure D-5 and Figure D-6 show an ANOA example vessel element detail and ANOA example port element detail, respectively.

```
<?xml version="1.0" encoding="UTF-8"?>
<md:payloadFocus
        xsi:schemaLocation="../0.90/miem.xsd"
        xmlns:md="http://miem.gov/md"
        xmlns:sec="urn:us:gov:ic:ism:v2"
        xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">

        <md:section sectionPurpose="assertion">
                <md:element>
                        < md:noticeOfArrival />
                </md:element>
        </md:section>
        <md:section sectionPurpose="reference objects">
                <md:element>
                        <!--Vessel Definition-->
                </md:element>
        </md:section>
        <md:section sectionPurpose="reference objects">
                <md:element>
                        <!--Port Definitions-->
                </md:element>
        </md:section>
        <md:section sectionPurpose="reference objects">
                <md:element>
                        <!--People Definitions-->
                </md:element>
        </md:section>
        <md:section sectionPurpose="reference objects">
                <md:element>
                        <!--Shipment Definitions-->
                </md:element>
        </md:section>
        <md:section sectionPurpose="reference objects">
                <md:element>
                        <!--Organization Definitions-->
                </md:element>
        </md:section>
</md:payloadFocus>
```

Figure D-3. Basic ANOA message structure.

```
<md:section sectionPurpose="assertion">
        <md:element>
                <md:noticeOfArrival md:id="NoticeID_0000">
                        <md:version value="2.4"/>
                        <md:creationTime>
                                <md:dateTime>2004-03-29T10:19:08</md:dateTime>
                        </md:creationTime>
                        <md:POC>
                                <md:entity>
                                        <md:organization md:ref="POCParty"/>
                                </md:entity>
                        </md:POC>
                        <md:submission>
                                <md:receiveTime>
                                        <md:dateTime>2007-12-27T08:00:00</md:dateTime>
                                </md:receiveTime>
                                <md:submitter>
                                        <md:organization md:ref="submittingParty"/>
                                </md:submitter>
                        </md:submission>

                        <md:vessel md:ref="ARR3232"/>
                        <md:noticeTransactionType>Initial</md:noticeTransactionType>
                        <md:noticeType>Arrival</md:noticeType>

                </md:noticeOfArrival>
        </md:element>
</md:section>
```

Figure D-4. ANOA Notice of Arrival message body.

```
<!--Vessel reference object -->
<md:section sectionPurpose="reference objects">
<md:element>
        <md:vessel md:id="ARR3232">
                <md:metadata>
                        <!-- OCE Information Goes Here -->
                        <md:comment value="Operational Condition of Equipment: Operational" />
                </md:metadata>
                <md:name value="Atlantic Light"/>
                <md:callSign value="XXX33421"/>
                <md:flag>
                        <md:name name="UNITED STATES"/>
                        <md:countryCode code="USA" />
                </md:flag>
                <!--IMO is here just to show that we can send one-->
                <md:IMO/>
                <md:officialCGNumber value="ARR3232"/>
                <md:classificationSociety value="U.S. Coast Guard"/>
                <md:ISMCode/>

                <md:cargo md:ref="Shipment" />

                <md:CDCOnBoard value="true" />

                <md:kinematics>
                        <md:position>
                                <md:latitude degs="20" mins="44" secs="21" UOM="dms"/>
                                <md:longitude degs="21" mins="06" secs="50" UOM="dms"/>
                        </md:position>
                        <md:location>
                                <md:nameDescription value="At Sea"/>
                        </md:location>
                </md:kinematics>

                <md:portOfCallHistory>
                        <!--Previous Foreign Port History - simple list-->
                        <md:pastPortOfCall>
                                <md:ATA><md:date>2003-03-20</md:date></md:ATA>
                                <md:ATD><md:date>2003-03-25</md:date></md:ATD>
                                <md:portIdentification md:ref="BingBong" />
                        </md:pastPortOfCall>
                        <!--Full list omitted, see Appendix D-->
                </md:portOfCallHistory>
```

Figure D-5. ANOA example vessel element detail.

```
<md:voyageHistory>                    <md:number value="1" />
    <md:type value="non-US to US" />
    <md:destination>
        <md:ETA>
            <md:dateTime>2004-04-01T06:00:00</md:dateTime>
        </md:ETA>
        <md:ETD>
            <md:dateTime>2004-04-02T08:15:00</md:dateTime>
        </md:ETD>
        <md:portIdentification md:ref="Baltimore"/>
    </md:destination>
    <md:pastPortOfCall>
        <md:metadata>
            <md:comment value="Last Port" />
        </md:metadata>
        <md:ATA><md:date>2004-03-20</md:date></md:ATA>
        <md:ATD><md:date>2003-03-21</md:date></md:ATD>
        <md:portIdentification md:ref="Aberdeen" />
    </md:pastPortOfCall>
    <md:nextPortOfCall>
        <md:ETA/>
        <md:portIdentification/>
    </md:nextPortOfCall>
</md:voyageHistory>

<md:charterer>
    <md:organization>
        <md:name value="Test Charterer"/>
    </md:organization>
</md:charterer>
<md:operator>
    <md:person>
        <md:name>
            <md:fullName value="John Test"/>
        </md:name>
    </md:person>
</md:operator>
<md:owner>
    <md:person>
        <md:name>
            <md:fullName value="John Test"/>
        </md:name>
    </md:person>
</md:owner>
```

Figure D-5. ANOA example vessel element detail (Continued).

```
        <md:personsOnBoard>
            <md:crewMember>
                <md:debarkInformation>
                    <md:date><md:date>2004-07-01</md:date></md:date>
                    <md:location>
                        <md:referenceObject>
                            <md:port md:ref="Miami" />
                        </md:referenceObject>
                    </md:location>
                </md:debarkInformation>
                <md:embarkInformation>
                    <md:date><md:date>2003-07-01</md:date></md:date>
                    <md:location>
                        <md:referenceObject>
                            <md:port md:ref="Miami" />
                        </md:referenceObject>
                    </md:location>
                </md:embarkInformation>
                <md:person md:ref="Crew1" />
                <md:crewRole role="Captain" />
            </md:crewMember>
            <md:crewmember />
            <md:passenger />
            <md:passenger />
        </md:personsOnBoard>

        <md:documentOfComplianceCertificate />
        <md:ISSC />
        <md:safetyManagementCertificate />
    </md:vessel>
```

Figure D-5. ANOA example vessel element detail (Continued).

```
<!--Port reference objects -->
<md:section sectionPurpose="reference objects">
<md:element>
    < md:port md:id="Baltimore">
        <md:code/>
        <md:name value="Baltimore" />
        <md:location>
            <md:address>
                <md:city value="Baltimore" />
                <md:countryCode code="USA" />
                <md:country value="United States"/>
                <md:stateProvince value="Maryland" />
            </md:address>
            <md:geographicDescription value="Inner Harbor" />
        </md:location>
        <md:subFacility>
            <md:facility>
                <md:name value="Facility 456" />
            </md:facility>
        </md:subFacility>
        <md:anchorage value="Anchorage 123" />
    </md:port>
</md:element>
<md:element>
    < md:port md:id="Aberdeen">
        <md:code value="ABD" />
        <md:name value="Aberdeen" />
        <md:location>
            <md:address>
                <md:city value="" />
                <md:countryCode code="GBR" />
                <md:country name="UNITED KINGDOM"/>
                <md:stateProvince/>
            </md:address>
            <md:geographicDescription value="Aberdeen Harbor" />
        </md:location>
    </md:port>
</md:element>
<!--For as many ports as necessary, one in each element -->
</md:section>
```

Figure D-6. ANOA example port element detail.

.1.1.2 *MIEM Schema Conceptual Diagram for ANOA*

Figure D-7 shows the MIEM schema conceptual diagram for ANOA.

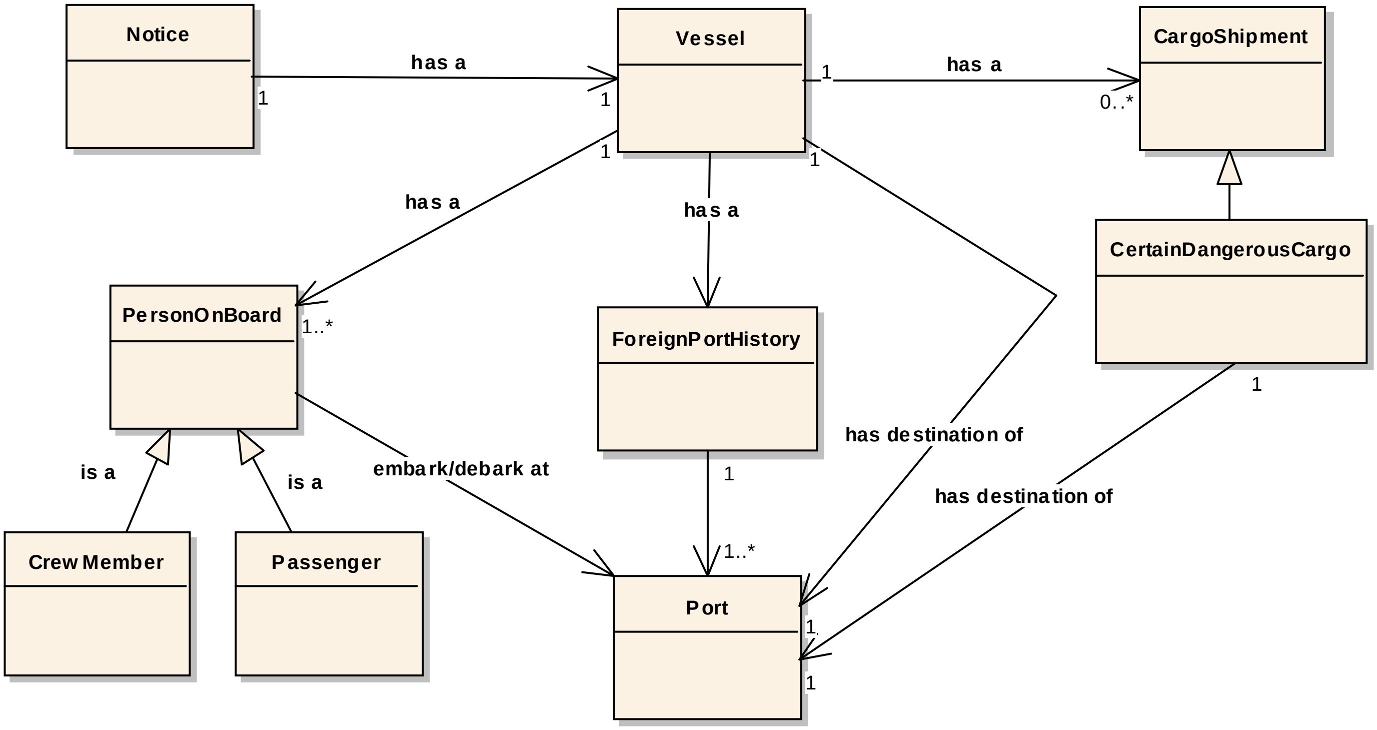


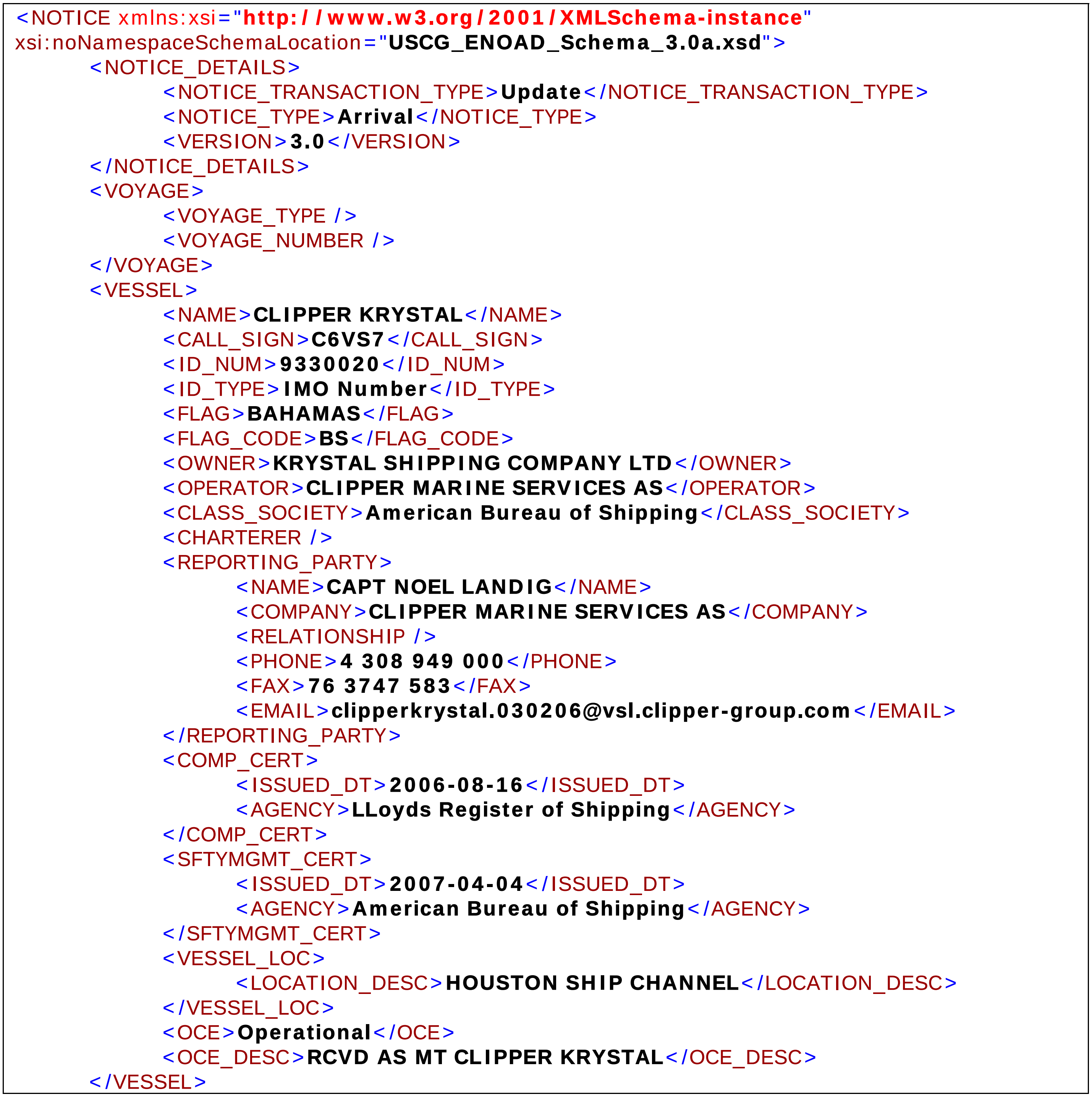
Figure D-7. MIEM – ANOA schema conceptual model.

.1.2 SANS Schema

The SANS schema (e-NOA) can be found by visiting the USCG NVMC at the following link.

http://www.nvmc.uscg.gov/nvmc/Items.aspx?id=7

Figure D-8 provides an example SANS message.



```
<NOTICE xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:noNamespaceSchemaLocation="USCG_ENOAD_Schema_3.0a.xsd">
        <NOTICE_DETAILS>
                <NOTICE_TRANSACTION_TYPE>Update</NOTICE_TRANSACTION_TYPE>
                <NOTICE_TYPE>Arrival</NOTICE_TYPE>
                <VERSION>3.0</VERSION>
        </NOTICE_DETAILS>
        <VOYAGE>
                <VOYAGE_TYPE />
                <VOYAGE_NUMBER />
        </VOYAGE>
        <VESSEL>
                <NAME>CLIPPER KRYSTAL</NAME>
                <CALL_SIGN>C6VS7</CALL_SIGN>
                <ID_NUM>9330020</ID_NUM>
                <ID_TYPE>IMO Number</ID_TYPE>
                <FLAG>BAHAMAS</FLAG>
                <FLAG_CODE>BS</FLAG_CODE>
                <OWNER>KRYSTAL SHIPPING COMPANY LTD</OWNER>
                <OPERATOR>CLIPPER MARINE SERVICES AS</OPERATOR>
                <CLASS_SOCIETY>American Bureau of Shipping</CLASS_SOCIETY>
                <CHARTERER />
                <REPORTING_PARTY>
                        <NAME>CAPT NOEL LANDIG</NAME>
                        <COMPANY>CLIPPER MARINE SERVICES AS</COMPANY>
                        <RELATIONSHIP />
                        <PHONE>4 308 949 000</PHONE>
                        <FAX>76 3747 583</FAX>
                        <EMAIL>clipperkrystal.030206@vsl.clipper-group.com</EMAIL>
                </REPORTING_PARTY>
                <COMP_CERT>
                        <ISSUED_DT>2006-08-16</ISSUED_DT>
                        <AGENCY>LLoyds Register of Shipping</AGENCY>
                </COMP_CERT>
                <SFTYMGMT_CERT>
                        <ISSUED_DT>2007-04-04</ISSUED_DT>
                        <AGENCY>American Bureau of Shipping</AGENCY>
                </SFTYMGMT_CERT>
                <VESSEL_LOC>
                        <LOCATION_DESC>HOUSTON SHIP CHANNEL</LOCATION_DESC>
                </VESSEL_LOC>
                <OCE>Operational</OCE>
                <OCE_DESC>RCVD AS MT CLIPPER KRYSTAL</OCE_DESC>
        </VESSEL>
```

Figure D-8. SANS e-NOA example message.

```
<ARRIVE_DEPART>
    <ARRIVE>
        <ARRIVE_DT>2009-01-10</ARRIVE_DT>
        <ARRIVE_TIME>13:00:00</ARRIVE_TIME>
        <PORT_OR_PLACE>Corpus Christi</PORT_OR_PLACE>
        <CITY>CORPUS CHRISTI</CITY>
        <STATE>TX</STATE>
        <FACILITY>FLINT HILLS RESOURCES</FACILITY>
        <ANCHORAGE>ARANSAS FAIRWAY ANCHORAGE</ANCHORAGE>
    </ARRIVE>
    <DEPART>
        <DEPART_DT>2009-01-11</DEPART_DT>
        <DEPART_TIME>15:00:00</DEPART_TIME>
    </DEPART>
    <CONTACT>
        <NAME>CALE KARRICK</NAME>
        <COMPANY>TEXAS MARINE AGENCY</COMPANY>
        <PHONE>361 877 3387</PHONE>
        <FAX>361 387 4395</FAX>
        <EMAIL>tma@tma-usgulf.com</EMAIL>
    </CONTACT>
</ARRIVE_DEPART>
<CARGO>
    <GENERAL_DESC>01/10/2009 CORPUS CHRISTI, TX — NIL</GENERAL_DESC>
    <CDC_ON_BOARD>No</CDC_ON_BOARD>
</CARGO>
<CDC_LIST />
<PREVIOUS_FOREIGN_PORT_LIST>
    <PREVIOUS_FOREIGN_PORT>
        <ARRIVAL_DT>2009-01-06</ARRIVAL_DT>
        <DEPARTURE_DT>2009-01-09</DEPARTURE_DT>
        <PREVIOUS_COUNTRY>N/A</PREVIOUS_COUNTRY>
        <PREVIOUS_COUNTRY_CODE>N/A</PREVIOUS_COUNTRY_CODE>
        <PREVIOUS_PLACE>Houston - ITC Dock 2 , DEERPARK, HOUSTON -
        UNITED STATES</PREVIOUS_PLACE>
    </PREVIOUS_FOREIGN_PORT>
    <PREVIOUS_FOREIGN_PORT>
        <ARRIVAL_DT>2008-11-12</ARRIVAL_DT>
        <DEPARTURE_DT>2008-11-13</DEPARTURE_DT>
        <PREVIOUS_COUNTRY>N/A</PREVIOUS_COUNTRY>
        <PREVIOUS_COUNTRY_CODE>N/A</PREVIOUS_COUNTRY_CODE>
        <PREVIOUS_PLACE>MISSISSUAGA - CANADA</PREVIOUS_PLACE>
    </PREVIOUS_FOREIGN_PORT>
    <PREVIOUS_FOREIGN_PORT>
        <ARRIVAL_DT>2008-10-25</ARRIVAL_DT>
        <DEPARTURE_DT>2008-10-27</DEPARTURE_DT>
        <PREVIOUS_COUNTRY>N/A</PREVIOUS_COUNTRY>
        <PREVIOUS_COUNTRY_CODE>N/A</PREVIOUS_COUNTRY_CODE>
        <PREVIOUS_PLACE>LAVERA - FRANCE</PREVIOUS_PLACE>
    </PREVIOUS_FOREIGN_PORT>
</PREVIOUS_FOREIGN_PORT_LIST>
```

Figure D-8. SANS e-NOA example message (Continued).

```
<CREW_LIST>
        <CREW>
                <POSITION>N/A</POSITION>
                <LAST_NAME>N/A</LAST_NAME>
                <FIRST_NAME>N/A</FIRST_NAME>
                <BIRTH_DT>9999-01-01</BIRTH_DT>
                <GENDER>Male</GENDER>
                <NATIONALITY>UNITED STATES</NATIONALITY>
                <NATIONALITY_CODE>US</NATIONALITY_CODE>
                <COUNTRY_RESIDENCE>UNITED STATES</COUNTRY_RESIDENCE>
                <COUNTRY_RESIDENCE_CODE>US</COUNTRY_RESIDENCE_CODE>
                <ID_TYPE>SSN</ID_TYPE>
                <ID_NUM>000-00-0000</ID_NUM>
                <EMBARK_COUNTRY>UNITED STATES</EMBARK_COUNTRY>
                <EMBARK_COUNTRY_CODE>US</EMBARK_COUNTRY_CODE>
                <EMBARK_DATE>9999-01-01</EMBARK_DATE>
        </CREW>
</CREW_LIST>
<Expansion>
        <Data_Field>
                <Name>Magnet_Notice_ID</Name>
                <Data_Type>2</Data_Type>
                <Data_Content>1661991</Data_Content>
        </Data_Field>
        <Data_Field>
                <Name>Submitted_Date</Name>
                <Data_Type>3</Data_Type>
                <Data_Content>2009-01-09</Data_Content>
        </Data_Field>
        <Data_Field>
                <Name>Submitted_Time</Name>
                <Data_Type>4</Data_Type>
                <Data_Content>18:40:01</Data_Content>
        </Data_Field>
        <Data_Field>
                <Name>Updated_Date</Name>
                <Data_Type>3</Data_Type>
                <Data_Content>2009-01-09</Data_Content>
        </Data_Field>
        <Data_Field>
                <Name>Updated_Time</Name>
                <Data_Type>4</Data_Type>
                <Data_Content>18:46:56</Data_Content>
        </Data_Field>
        <Data_Field>
                <Name>Arrival_Cotp_Id</Name>
                <Data_Type>2</Data_Type>
                <Data_Content>22</Data_Content>
        </Data_Field>
```

Figure D-8. SANS e-NOA example message (Continued).

```
        <Data_Field>
            <Name>Arrival_Cotp_Name</Name>
            <Data_Type>1</Data_Type>
            <Data_Content>Sector Corpus Christi</Data_Content>
        </Data_Field>
        <Data_Field>
            <Name>Arrival_UN_Locode</Name>
            <Data_Type>1</Data_Type>
            <Data_Content />
        </Data_Field>
        <Data_Field>
            <Name>Num_Suppress_Arrivals</Name>
            <Data_Type>2</Data_Type>
            <Data_Content>1</Data_Content>
        </Data_Field>
        <Data_Field>
            <Name>Num_Suppress_Previous_Foreign_Ports</Name>
            <Data_Type>2</Data_Type>
            <Data_Content>1</Data_Content>
        </Data_Field>
    </Expansion>
</NOTICE>
```

Figure D-8. SANS e-NOA example message (Continued).

.1.3 SILO Schema

SILO provides a single aggregate VOI list using the community-defined MIEM format and the Bi-Nation VOI Lexicon. Figure D-9 shows the conceptual model of SILO. Figure D-10 shows the basic SILO message structure.

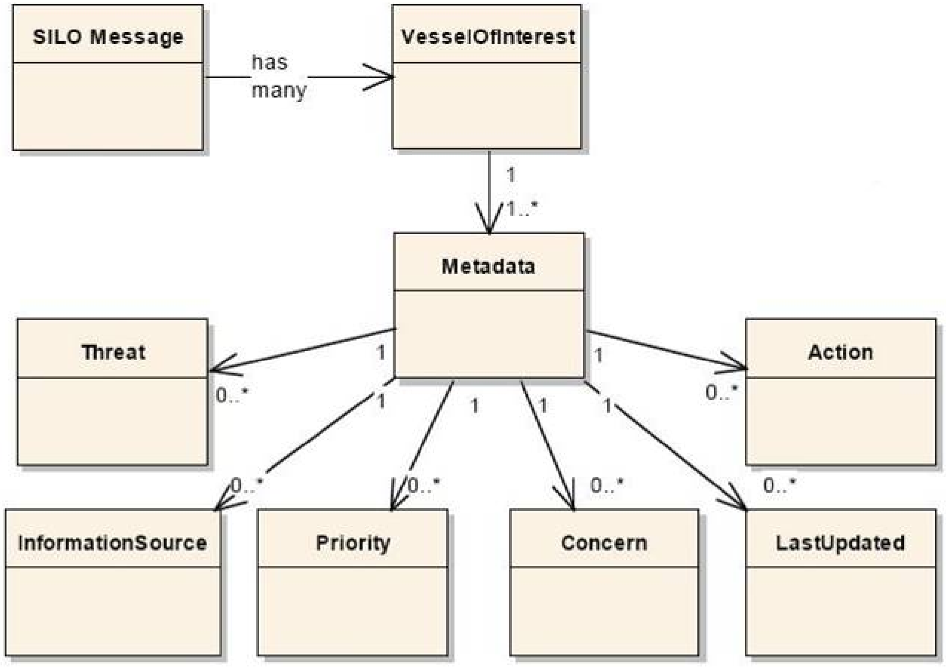
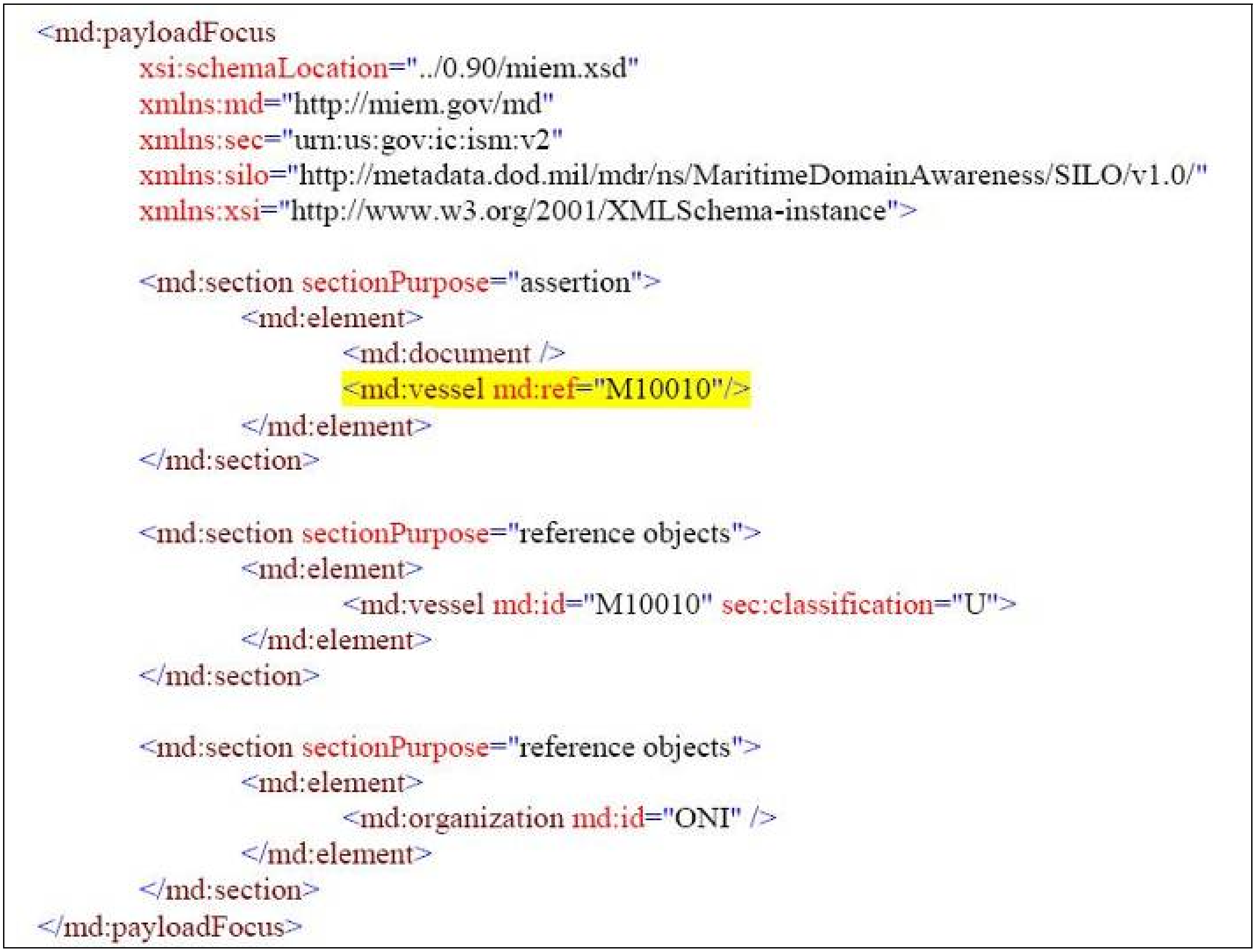


Figure D-9. SILO conceptual model.



```
<md:payloadFocus
        xsi:schemaLocation="../0.90/miem.xsd"
        xmlns:md="http://miem.gov/md"
        xmlns:sec="urn:us:gov:ic:ism:v2"
        xmlns:silo="http://metadata.dod.mil/mdr/ns/MaritimeDomainAwareness/SILO/v1.0/"
        xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">

        <md:section sectionPurpose="assertion">
                <md:element>
                        <md:document />
                        <md:vessel md:ref="M10010"/>
                </md:element>
        </md:section>

        <md:section sectionPurpose="reference objects">
                <md:element>
                        <md:vessel md:id="M10010" sec:classification="U">
                </md:element>
        </md:section>

        <md:section sectionPurpose="reference objects">
                <md:element>
                        <md:organization md:id="ONI" />
                </md:element>
        </md:section>
</md:payloadFocus>
```

Figure D-10. Basic SILO message structure.

.2 Listing of Terms within ANOA Vocabulary

Note: Each term is listed in the order in which it appears within an ANOA message. Listings are not in alphabetical order. This table only calls out the terms from the MIEM which are used in the ANOA messages, and is not a complete listing of the terms available in the MIEM. Element definitions will not be repeated, even if reused. See the example message in this appendix for the complete message structure.

Term	Definition
payloadFocus	The root element of a MIEM message.
section	A logical grouping element within a MIEM message. A payloadFocus element can contain any number of these.
element	An information container element in MIEM. A section can contain any number of these. A single element can contain only one top-level MIEM element.
noticeOfArrival	The top-level element containing the ANOA message.
version	The version of the electronic Notice of Arrival/Departure (e-NOA/D) schema from which this ANOA message has been generated.
creationTime	The time of the creation of this instance of the ANOA message.
POC	A point of contact element.
entity	An entity. This element can either contain a number of sub-elements representing the entity, or a reference to an entity defined elsewhere in the document.
submission	A metadata element wrapping elements that describe the document.
receiveTime	The time of the reception of this ANOA message from the vessel.
submitter	This element can contain sub-elements that describe the submitter of this document, or a reference to this information elsewhere in the document.
vessel	An element containing all the sub-elements describing a vessel. For ANOA purposes, this is a reference to a complete vessel element elsewhere in the document.
noticeTransactionType	This is a codelist element describing the type of e-NOA/D message, either Initial or Update.
noticeType	Codelist element describing whether this message is an arrival notice or a departure notice.
metadata	An element that can contain a number of other metadata elements.
comment	Used in the ANOA to describe the Operational Condition of Equipment (OCE) in the vessel element.
name	The name of the vessel.
callSign	The call sign of the vessel.
flag	An element that contains elements that describe the flag under which this vessel sails.
name	Name of the country to which this flag belongs. This element is a codelist.
countryCode	Three letter country code. This element is a codelist.
IMO	The International Maritime Organization number of this vessel.
officialCGNumber	The U.S. Coast Guard number of this vessel.
MMSI	The Maritime Mobile Service Identity of the vessel.
ISMCode	The International Safety Management code for the vessel.
cargo	An element containing all the elements describing a cargo shipment.
lastKnownState	An element that contains a number of sub-elements describing the last known state of the vessel, such as position, speed, and other temporal-dependent factors.

Term	Definition
CDCOnBoard	A true/false value indicating whether this vessel has certain dangerous cargo onboard.
kinematics	This element contains a number of sub-elements describing the position and motion of an object.
position	Contains elements that describe the absolute coordinates of an object.
latitude	Describes the latitude of an object in degrees, minutes, seconds (DMS).
longitude	Describes the longitude of an object in DMS.
location	Contains elements that allow the textual description of the location of an object.
nameDescription	Text label on the location of an object.
voyageHistory	Contains elements describing the voyage history of this vessel.
number	The voyage number of this voyage for this vessel.
type	The type of voyage, U.S. to non-U.S. or non-U.S. to U.S.
destination	Contains elements describing the destination of this vessel.
ETA	The Estimated Time of Arrival (ETA) for this vessel at this destination.
ETD	The Estimated Time of Departure (ETD) for this vessel from this destination.
portIdentification	A reference to a complete port element elsewhere in the document.
pastPortOfCall	A collection of elements describing a past port of call for this vessel.
ATA	Actual Time of Arrival (ATA).
ATD	Actual Time of Departure (ATD).
nextPortOfCall	A collection of elements describing the next port of call for this vessel.
portOfCallHistory	A collection of pastPortOfCall elements that record the past ports this vessel has visited.
charterer	An element describing the entity who chartered this vessel.
operator	An element describing the entity responsible for operating this vessel.
owner	An element describing the entity who owns this vessel.
personsOnBoard	A collection of person elements describing the crew and non-crew onboard this vessel.
crewMember	A collection of elements describing a crewmember on this vessel.
debarkInformation	A collection of elements about the debark location for this person.
embarkInformation	A collection of elements about the embark location for this person.
person	A reference to a complete person object elsewhere in the document.
crewRole	A text field describing the role of this person in the crew.
passenger	A collection of elements describing a passenger on this vessel.
documentOfComplianceCertificate	A collection of elements describing this vessel’s compliance certificate.
expirationDate	The date this certificate expires.
issueDate	The data this certificate was issued.
issuingAgency	A collection of elements describing the entity who issued this document.
ISSC	A collection of elements describing the International Ship Security Certificate (ISSC) for this vessel.
interimReason	A reason field in the case that ISSCType is Interim.
ISSCType	The type of the ISSC; e.g., Interim.
recognizedSecurity	A collection of elements describing the recognized security organization or flag administration.
government	A collection of elements describing a government.
securityOfficerPOC	A point of contact serving as the security officer for ISSC purposes.
contactNumber	An element containing the number/type elements that describe a phone number.
number	A phone number represented as a string.
phoneType	Describes the type of phone number; e.g., “voice” or “fax.”
email	An email address.

Term	Definition
VSPImplemented	A true/false value indicating whether a Vessel Security Plan has been implemented.
safetyManagementCertificate	A collection of elements representing the safety management certificate for this vessel.
port	A collection of elements describing a port.
code	The international 3-letter port code.
address	A collection of fields describing an address.
city	The name of the city in the address.
stateProvince	The name of the state or province in the address.
subFacility	A collection of elements that describe a facility.
anchorage	A text field that can be used to describe an anchorage.
name	A collection of elements describing a person's name.
familyName	The family name of a person.
givenName	The given name of a person.
middleName	The middle name of a person.
nationality	A collection of elements describing a person's nationality.
name	A codelist of countries.
countryCode	A codelist of 3-letter country codes.
marinersDoc	A collection of elements describing this person's Mariner's Document.
identification	A document specific ID string.
gender	The person's gender.
birthDate	The person's date of birth.
homeLocation	A collection of elements describing the home location of this person, which can also be country of origin.
cargoShipment	A MIEM primary maritime element used to describe a cargo shipment.
otherShipmentIdentifier	A free text field used to describe the shipment; e.g., "Bulk Pig Iron" or "Manufactured Goods."
hazmatDeclaration	A collection of elements describing the specifics of a single kind of hazardous material (hazmat) or certain dangerous cargo.
amount	Free text field used to specify amount of hazmat cargo; e.g., "80 tons" or "500 liters."
chemicalCommonName	Common name of the chemical/chemicals in this hazmat cargo.
destination	The final destination of this hazmat/certain dangerous cargo (CDC).
UNHazmatCode	United Nations hazmat code number for this specific type of cargo.
organization	A collection of elements describing an organization, which can be a person, company, etc.
name	The common name of the organization.

This page intentionally left blank.

APPENDIX E. SERVICES

E.1 NCES

NCES is the Core Enterprise Service component that is a part of the Net-Centric Warfare GIG Enterprise Services for DISA. NCES mission is to enable warfighting, intelligence, and business systems. The concept is to migrate from system-focused stove-piped systems to a network and data centric model.

There are several services that NCES provides; the following are the services that the MDA DS COI leverages.

E.1.1 Service Security

NCES Service Security enables secure web-services interactions and enables the exposure of data and services to users. NCES Service Security enables programs using NCES to perform with the level of security appropriate to their function and needs. NCES provides the architecture for authentication, authorization, confidentiality, message integrity, non-repudiation, manageability, and accountability. NCES enables more agile and rapid fielding of service capabilities, and reduces the cost of fielding the services, by specifying a common architecture and providing shared supporting services. Through flexible security options, NCES enables the users to apply the appropriate security. These interoperable NCES security mechanisms are intended to be the used by the DOD business, intelligence, and warfighting communities.

NCES is primarily addressing web services security by:

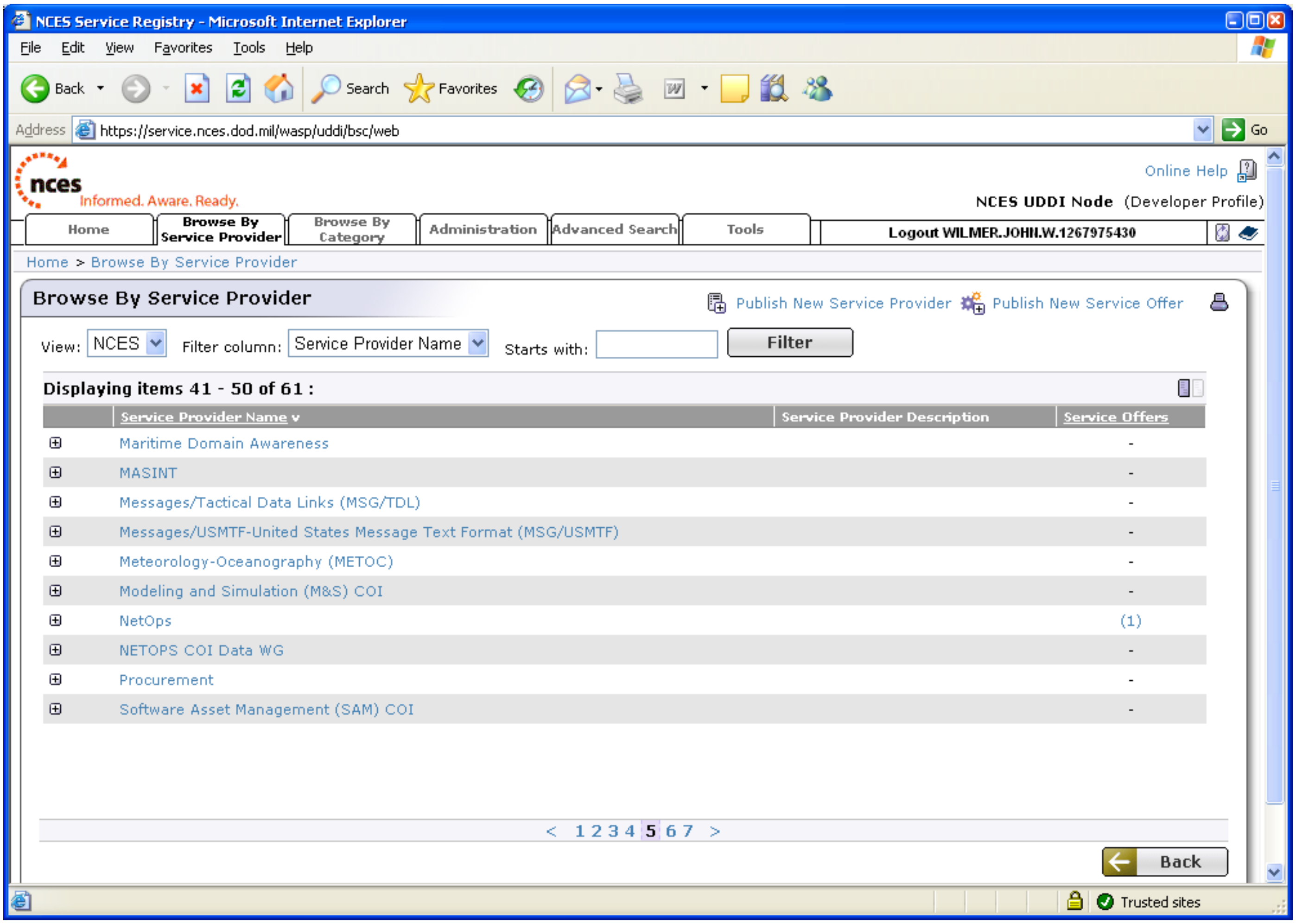
- Providing an enterprise Robust Certificate Validation Service (RCVS) to support effective authentication of both individuals and web services, allowing clients to delegate certificate validation tasks, in part or in whole, which is especially useful when the client side does not have the capability for PKI processing.
- Providing an enterprise Attribute Service (AS) to support centralized retrieval of authoritative attribute values for individuals, primarily to support authorization of users without pre-provisioned accounts ("unanticipated users") of web services.
- Providing a SOAP message interface specification that helps ensure interoperability of the use of accepted standards for ensuring confidentiality, integrity, and non-repudiation of message contents.

Other security offerings include:

- A conformance test kit (CTK) that verifies that the web service is able to securely communicate with other web services using the NCES SOAP message interface specification.
- A commercial off-the-shelf (COTS) interoperability list of products that are known to comply with the NCES SOAP message interface specification.
- Implementation guidance with examples of how to implement security in the enterprise and local enclaves.

E.1.2 Service Discovery

A key component of a service-enabled Environment is a registry (Figure E-1) containing information about the services which make up that environment. This registry not only provides a catalog of services, it provides important information about the provider of the service, the functionality of the service, service interface details, and service categorization information. This "service registry" is intended to provide all of the information required for a application developer to locate an appropriate service; determine the features and functions provided by that service; identify how to invoke the service; and determine where that service resides. The NCES Service Discovery provides such a service registry.


NCES Service Registry - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back
Search
Favorites
Address https://service.nces.dod.mil/wasp/uddi/bsc/web
Go
nces
Informed. Aware. Ready.
Online Help
NCES UDDI Node (Developer Profile)
Home
Browse By Service Provider
Browse By Category
Administration
Advanced Search
Tools
Logout WILMER.JOHN.W.1267975430
Home > Browse By Service Provider
Publish New Service Provider
Publish New Service Offer
Filter
< 1 2 3 4 5 6 7 >
Back
Trusted sites

Browse By Service Provider

View: NCES Filter column: Service Provider Name Starts with:

Displaying items 41 - 50 of 61 :

	Service Provider Name v	Service Provider Description	Service Offers
⊞	Maritime Domain Awareness		-
⊞	MASINT		-
⊞	Messages/Tactical Data Links (MSG/TDL)		-
⊞	Messages/USMTF-United States Message Text Format (MSG/USMTF)		-
⊞	Meteorology-Oceanography (METOC)		-
⊞	Modeling and Simulation (M&S) COI		-
⊞	NetOps		(1)
⊞	NETOPS COI Data WG		-
⊞	Procurement		-
⊞	Software Asset Management (SAM) COI		-

Figure E-1. NCES service registry website.

NCES Service Discovery (https://service.nces.dod.mil/wasp/uddi/bsc/web) allows organizations that provide Web services on the NIPRNET or SIPRNET to publish and advertise those services in an "enterprise" registry. Service Discovery provides a user interface for "service providers" to enter or publish information related to their Web services. This user interface has been customized to provide appropriate governance during the publishing process to ensure the validity of the information being entered and to include adequate categorization information to enable successful discovery of the published services.

NCES Service Discovery enables “service consumers” to discover Web services that are available on the NIPRNET or SIPRNET. Typically, a service consumer will be an application designer or developer who is interested in using existing services and searches for these services at “design time.” NCES Service Discovery provides an appropriate user interface for the “design time” discovery of published services. Services can also be discovered at “runtime,” enabling an application to dynamically discover the existence of a service or invoke a service endpoint at runtime. NCES Service Discovery also supports this type of “runtime” discovery, via a standard UDDI Inquiry Web service.

E.1.3 Metadata Discovery

Metadata services provide the ability for DoD Enterprise systems to discover and manage (publish, make visible, and access) various metadata artifacts critical to a system’s and/or person’s ability to exchange and understand data components within the enterprise. They provide visibility of data representations and enable the development and management of data products to support mediation capabilities within the enterprise. Metadata Discovery is accomplished through the use of the DoD Metadata Registry (MDR) (Figure E-2) (https://metadata.dod.mil). This provides an on-line repository based on e-business XML (ebXML) which enables developers to reuse, understand, integrate with, and share existing data assets (metadata). Having the MDR enables the reuse and governance of data asses and allows COI data to persist after the COI is disbanded. The target datasets include web services, databases, and vocabularies. The MDR also provides a portal for developers to access the information, and provides web services for machine-to-machine access. The MDR serves the DoD, DHS, IC, National Aeronautics and Space Administration (NASA), and North Atlantic Treaty Organization (NATO) and has over 900 Programs of Records supported. Access is available through single sign-on through Defense Knowledge Online (DKO).

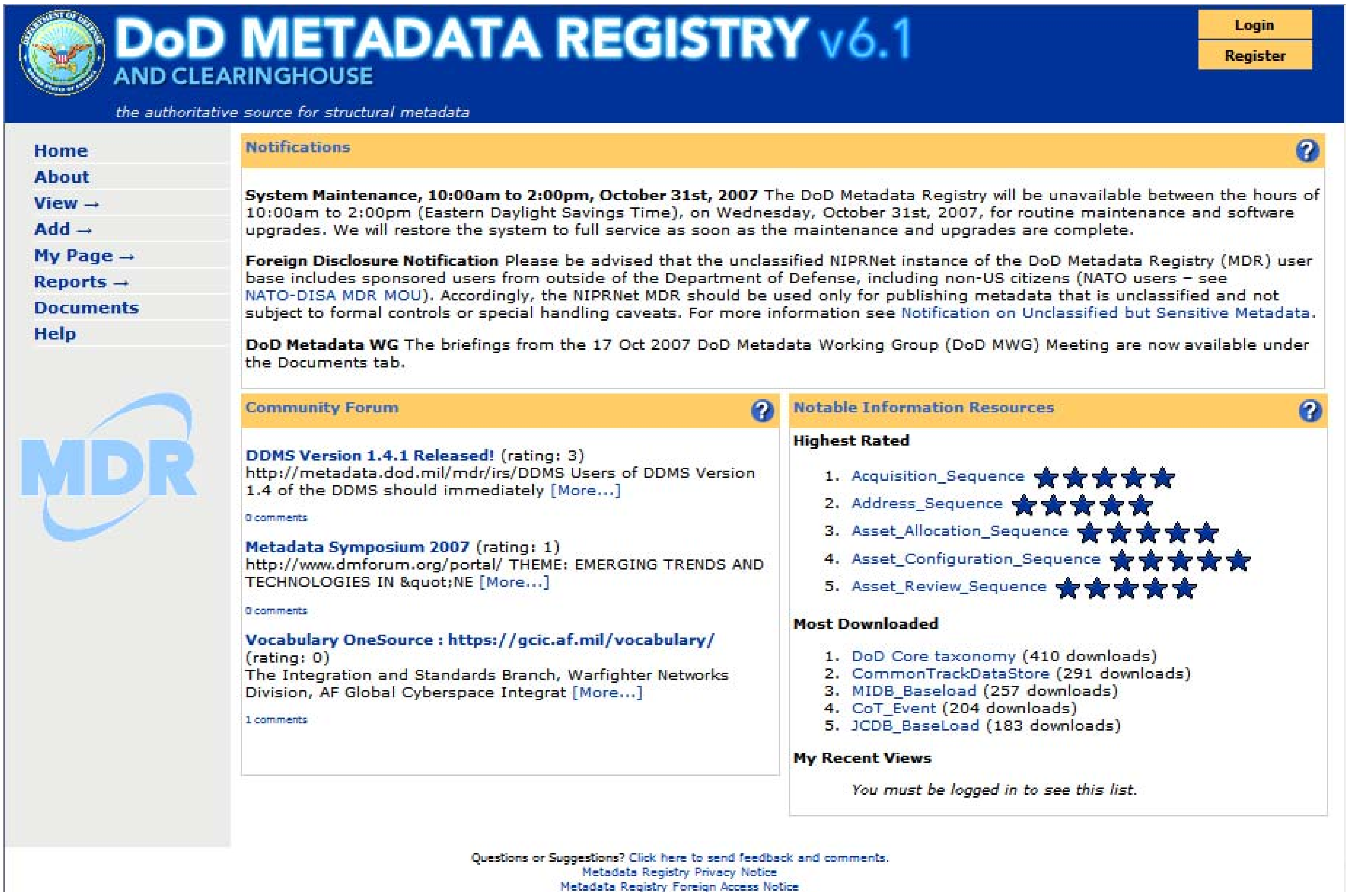
E.1.4 Machine to Machine Messaging

The Messaging Core Enterprise Service (CES) provides a federated, distributed, and fault-tolerant enterprise message bus. It provides the following services.

- Delivers high-performance, scalable, and interoperable asynchronous event notifications to both applications and end-users.
- Supports the configuration of Quality of Service (QoS) for a published message including the priority, precedence, and time-to-live (TTL).
- Provides guaranteed delivery to disconnected users or applications.
- Utilizes multiple message brokers, potentially within different administrative domains, to support the distributed, federated nature of the GIG.

The Messaging CES provides the following benefits:

- Promotes decoupling of information among producers and consumers.
  - Provides asynchronous point-to-multi-point (publish & subscribe).
  - Producers do not keep track of consumers.
  - Producers and consumers do not have to be continuously connected to network.
- Ensures QoS.
  - Provides guaranteed messaging.
  - Messages are queued for delivery.



Notifications

System Maintenance, 10:00am to 2:00pm, October 31st, 2007 The DoD Metadata Registry will be unavailable between the hours of 10:00am to 2:00pm (Eastern Daylight Savings Time), on Wednesday, October 31st, 2007, for routine maintenance and software upgrades. We will restore the system to full service as soon as the maintenance and upgrades are complete.

Foreign Disclosure Notification Please be advised that the unclassified NIPRNet instance of the DoD Metadata Registry (MDR) user base includes sponsored users from outside of the Department of Defense, including non-US citizens (NATO users – see NATO-DISA MDR MOU). Accordingly, the NIPRNet MDR should be used only for publishing metadata that is unclassified and not subject to formal controls or special handling caveats. For more information see Notification on Unclassified but Sensitive Metadata.

DoD Metadata WG The briefings from the 17 Oct 2007 DoD Metadata Working Group (DoD MWG) Meeting are now available under the Documents tab.

Community Forum

DDMS Version 1.4.1 Released! (rating: 3)
http://metadata.dod.mil/mdr/irs/DDMS Users of DDMS Version 1.4 of the DDMS should immediately [More...]

0 comments

Metadata Symposium 2007 (rating: 1)
http://www.dmforum.org/portal/ THEME: EMERGING TRENDS AND TECHNOLOGIES IN &quot;NE [More...]

0 comments

Vocabulary OneSource : https://gcic.af.mil/vocabulary/ (rating: 0)
The Integration and Standards Branch, Warfighter Networks Division, AF Global Cyberspace Integrat [More...]

1 comments

Notable Information Resources

Highest Rated

1. Acquisition_Sequence ★★★★★
2. Address_Sequence ★★★★★
3. Asset_Allocation_Sequence ★★★★★
4. Asset_Configuration_Sequence ★★★★★
5. Asset_Review_Sequence ★★★★★

Most Downloaded

1. DoD Core taxonomy (410 downloads)
2. CommonTrackDataStore (291 downloads)
3. MIDB_Baseload (257 downloads)
4. CoT_Event (204 downloads)
5. JCDB_BaseLoad (183 downloads)

My Recent Views

You must be logged in to see this list.

Questions or Suggestions? Click here to send feedback and comments.
Metadata Registry Privacy Notice
Metadata Registry Foreign Access Notice

Figure E-2. DoD metadata registry website.

- Provides mediation of message formats between COIs.
  - Allows for application integration.
  - Supports mediation/orchestration.

E.1.5 Content Discovery

NCES Content Discovery provides a capability for producers to expose content to the GIG for discovery by unanticipated consumers. It is composed of a set of Web applications and services that address the net-centric guiding principle of visibility, and is available in the SIPRNET and NIPRNET environments.

Users interact with Content Discovery primarily through two Web applications:

- Enterprise Search (https://search.ces.mil): A Web-based search application that includes content crawled by the centralized search engine, search results from federated search sources, and Enterprise Catalog results.
- Enterprise Catalog (https://catalog.ces.mil): A searchable catalog in which content owners publish discovery metadata that describes resources such as services, applications, databases, or documents.

There are two ways to interact with Content Discovery: as a search consumer or as a content provider.

As a search consumer, the NCES Content Discovery provides a single, simple user interface, consistent with commonly-used Internet search engines, that allows users to discover information from across the DoD.

Content Discovery provides three ways that content providers can expose their content, while controlling the visibility of sensitive information: Centralized Search, Federated Search, and the Enterprise Catalog. The MDA DS COI primarily uses Federated Search.

E.1.6 Enterprise Service Management

Enterprise Service Management (ESM) is the NCES component that provides Web service management. As the number of Web services deployed increase, the ability to effectively manage them becomes critical. Monitoring enterprise Web services allows service providers and service management administrators to collect and evaluate mission critical, service vital signs such as service performance metrics and QoS data. ESM integrates with several other service management offerings to provide extensive situational awareness.

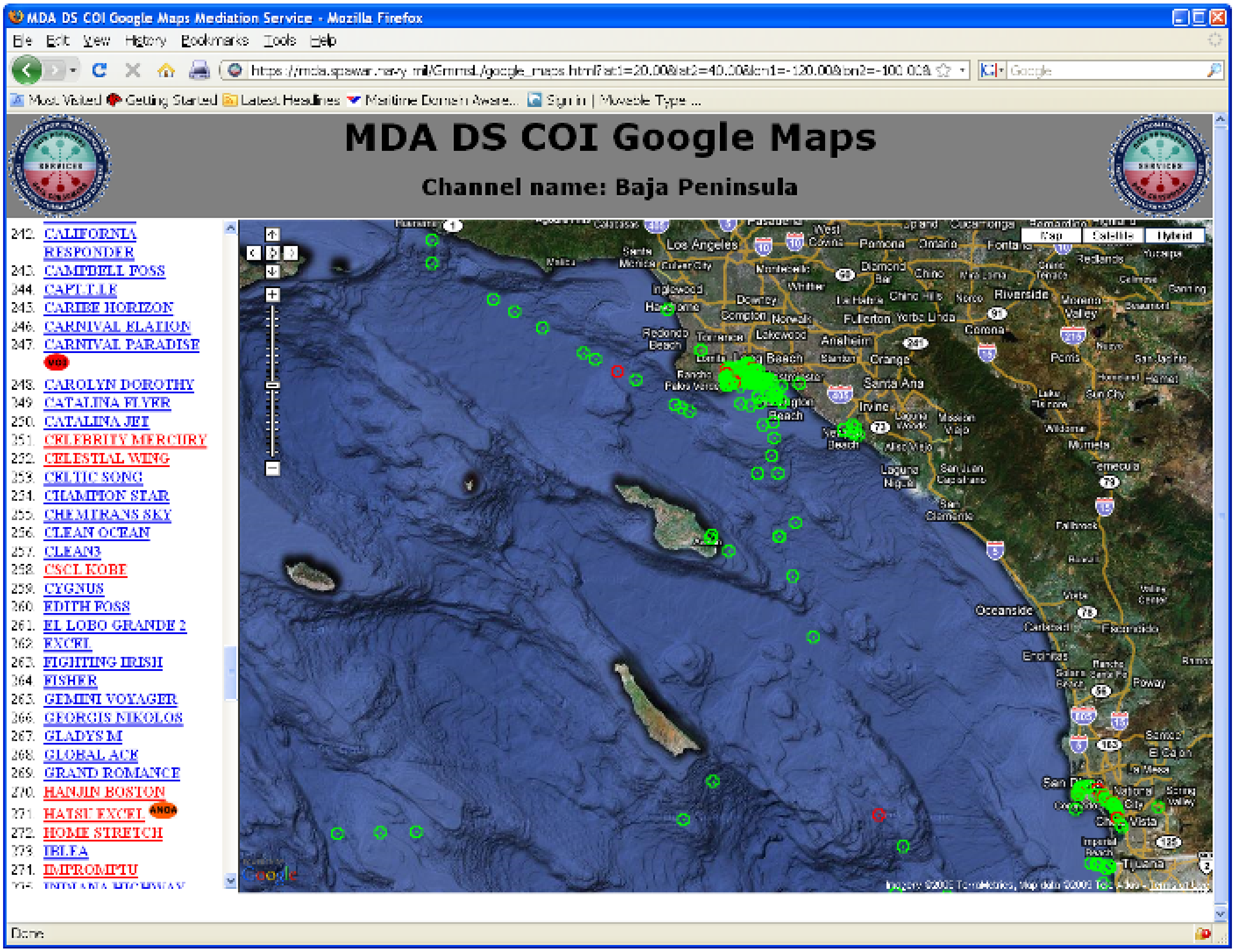
E.2 MDA DS COI Services

E.2.1 Google Maps Mediation Service (GMMS)

The MDA DS COI developed the GMMS to provide the unanticipated user that has a Common Access Card (CAC) access to MDA DS COI data such as AIS, ANOA, and SILO data. In Figure E-3, there is AIS positional information displayed on the map and indications of associated VOI and ANOA data with the “Carnival Paradise” and the “Hatsu Excel.” For more information and access, visit the SPAWAR development site at https://mda.spawar.navy.mil/GmmsL/gmaps.jsp. You may also access the operational GMMS site at https://mda.csd.disa.mil/GmmsL/gmaps.jsp.

E.2.2 Metrics Analysis Tool (MAT)

MAT was developed by the USCG R&DC Team for the MDA DS COI to capture, analyze, and display metrics information about the MDA DS COI data sharing efforts. The site includes service status monitoring, and detailed histories of metrics captured. For users with a CAC, visit https://dscoi3.rdc.uscg.gov/MAT (Figure E-4).



MDA DS COI Google Maps Mediation Service - Mozilla Firefox

File Edit View History Bookmarks Tools Help

https://mda.spawar.navy.mil/Gmms/google_maps.html?lat1=20.00&lat2=40.00&lon1=-120.00&lon2=-100.00&

Most Visited Getting Started Latest Headlines Maritime Domain Aware... Sign in | Movable Type ...

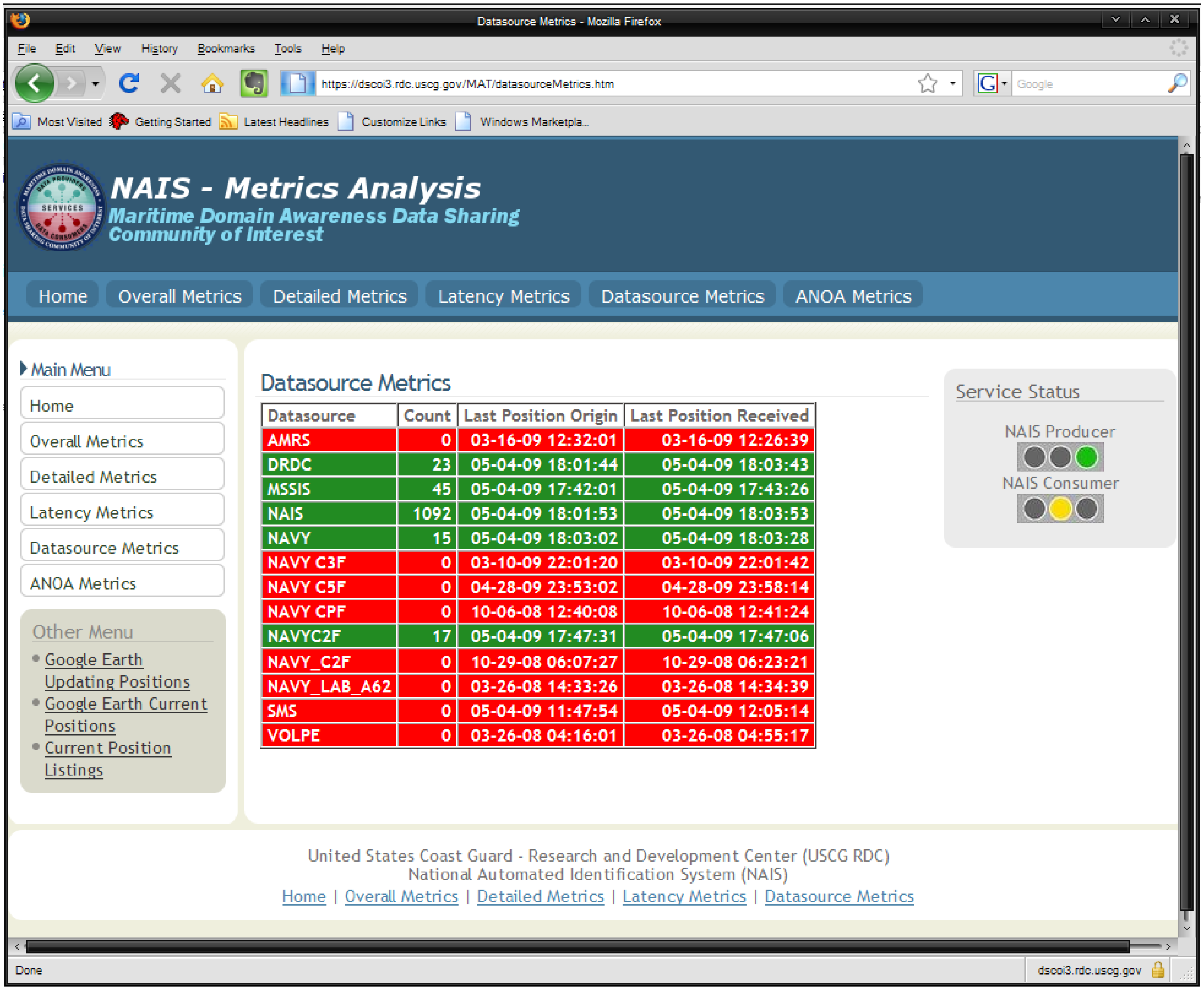
MDA DS COI Google Maps

Channel name: Baja Peninsula

242. CALIFORNIA RESPONDER
243. CAMPBELL FOSS
244. CAPELLE
245. CARIBE HORIZON
246. CARNIVAL ELATION
247. CARNIVAL PARADISE VOI
248. CAROLYN DOROTHY
249. CATALINA FLYER
250. CATALINA JET
251. CELEBRITY MERCURY
252. CELESTIAL WING
253. CELTIC SONG
254. CHAMPION STAR
255. CHEMTRANS SKY
256. CLEAN OCEAN
257. CLEAN3
258. CSCL KOBE
259. CYGNUS
260. EDITH FOSS
261. EL LOBO GRANDE 2
262. EXCEL
263. FIGHTING IRISH
264. FISHER
265. GEMINI VOYAGER
266. GEORGIS NIKOLOS
267. GLADYS M
268. GLOBAL ACE
269. GRAND ROMANCE
270. HANJIN BOSTON
271. HATSU EXCEL ANOA
272. HOME STRETCH
273. IBLEA
274. IMPROMPTU
275. INDIANA HIGHWAY

Done

Figure E-3. GMMS website.



NAIS - Metrics Analysis

Maritime Domain Awareness Data Sharing Community of Interest

Datasource Metrics

Datasource	Count	Last Position Origin	Last Position Received
AMRS	0	03-16-09 12:32:01	03-16-09 12:26:39
DRDC	23	05-04-09 18:01:44	05-04-09 18:03:43
MSSIS	45	05-04-09 17:42:01	05-04-09 17:43:26
NAIS	1092	05-04-09 18:01:53	05-04-09 18:03:53
NAVY	15	05-04-09 18:03:02	05-04-09 18:03:28
NAVY C3F	0	03-10-09 22:01:20	03-10-09 22:01:42
NAVY C5F	0	04-28-09 23:53:02	04-28-09 23:58:14
NAVY CPF	0	10-06-08 12:40:08	10-06-08 12:41:24
NAVYC2F	17	05-04-09 17:47:31	05-04-09 17:47:06
NAVY_C2F	0	10-29-08 06:07:27	10-29-08 06:23:21
NAVY_LAB_A62	0	03-26-08 14:33:26	03-26-08 14:34:39
SMS	0	05-04-09 11:47:54	05-04-09 12:05:14
VOLPE	0	03-26-08 04:16:01	03-26-08 04:55:17

Service Status

NAIS Producer ● ● ●

NAIS Consumer ● ● ●

United States Coast Guard - Research and Development Center (USCG RDC)
National Automated Identification System (NAIS)
Home | Overall Metrics | Detailed Metrics | Latency Metrics | Datasource Metrics

Figure E-4. MAT website.

This page intentionally left blank.